Bounds for algorithms in differential algebra [1]

Oleg Golubitsky [a,3] Marina Kondratieva [b] Marc Moreno Maza [c,4]
Alexey Ovchinnikov [d,2]

[a] *University of Western Ontario*
Department of Computer Science
London, Ontario, Canada N6A 5B7

[b] *Moscow State University*
Department of Mechanics and Mathematics
Leninskie gory, Moscow, Russia, 119992

[c] *University of Western Ontario*
Department of Computer Science
London, Ontario, Canada N6A 5B7

[d] *North Carolina State University*
Department of Mathematics
Raleigh, NC 27695-8205, USA

Abstract

We consider the Rosenfeld-Gröbner algorithm for computing a regular decomposition of a radical differential ideal generated by a set of ordinary differential polynomials in n indeterminates. For a set of ordinary differential polynomials F, let $M(F)$ be the sum of maximal orders of differential indeterminates occurring in F. We propose a modification of the Rosenfeld-Gröbner algorithm, in which for every intermediate polynomial system F, the bound $M(F) \leqslant (n-1)!M(F_0)$ holds, where F_0 is the initial set of generators of the radical ideal. In particular, the resulting regular systems satisfy the bound. Since regular ideals can be decomposed into characterizable components algebraically, the bound also holds for the orders of derivatives occurring in a characteristic decomposition of a radical differential ideal.

We also give an algorithm for converting a characteristic decomposition of a radical differential ideal from one ranking into another. This algorithm performs all differentiations in the beginning and then uses a purely algebraic decomposition algorithm.

Key words: differential algebra, characteristic sets, radical differential ideals, decomposition into regular components
1991 MSC: 12H05, 13N10, 13P10

1. Introduction

This paper is about constructive differential algebra. We study algorithms dealing with algebraic differential equations. Many different problems can be addressed to this topic. One can, for instance, test membership to a radical differential ideal, compute the Kolchin dimensional polynomial. The kind of algorithms we are dealing with are decomposition algorithms for radical differential ideals. Generally, there are two such algorithms, although they have variations.

The Ritt-Kolchin algorithm computes a prime decomposition of a radical differential ideal, where each prime component is represented by its characteristic set. This algorithm is based on important results in differential algebra (see Ritt (1950); Kolchin (1973)), such as the Basis Theorem, the Prime Decomposition Theorem for radical differential ideals, the differential version of the Hilbert Theorem of Zeroes, and the Rosenfeld Lemma. It also relies on the solution of the so-called factorization problem: given an autoreduced set, determine whether the corresponding algebraic saturated ideal is prime and, if it is not, find two polynomials outside of the ideal whose product belongs to the ideal.

Due to the complexity of the factorization problem, it was desirable to avoid it, which was done in the Rosenfeld-Gröbner algorithm proposed in (Boulier et al., 1995). Instead of decomposing a given radical differential ideal into prime components, this algorithm represents it as an intersection of regular differential ideals, also introduced in (Boulier et al., 1995); the correctness of the algorithm, in addition to the above-mentioned theorems, is provided by the Lazard Lemma, which states that regular ideals are radical. Four different proofs of this lemma can be found in (Boulier et al., 1997; Morrison, 1999; Hubert, 2000; Boulier et al., 2006).

The Rosenfeld-Gröbner algorithm is the first decomposition algorithm in differential algebra that has been actually implemented upto our knowledge. It forms an integral part of the `diffalg` package in the computer algebra system Maple. Updates of this package are available at `http://www-sop.inria.fr/cafe/Evelyne.Hubert/diffalg/`. A more efficient implementation of this algorithm in C language can be found at the website `http://www.lifl.fr/~boulier/BLAD/`.

Various improvements of the Rosenfeld-Gröbner algorithm have been proposed in (Boulier et al., 1997; Hubert, 2000, 2003, 2004; Bouziane et al., 2001). They all avoid the factorization problem and for this reason are called factorization-free methods in differential algebra. However, no theoretical bound for the computational complexity of any of these algorithms is known.

We make the first step towards the goal of estimating this complexity: we bound the orders of differential polynomials appearing in the computations. The main results of this

Email addresses: `oleg.golubitsky@gmail.com` (Oleg Golubitsky), `kondrmar@rol.ru` (Marina Kondratieva), `moreno@orcca.on.ca` (Marc Moreno Maza), `aiovchin@ncsu.edu` (Alexey Ovchinnikov).

URLs: `http://www.cs.queensu.ca/~golub/` (Oleg Golubitsky), `http://shade.msu.ru/~kondra_m/` (Marina Kondratieva), `http://www.csd.uwo.ca/~moreno/` (Marc Moreno Maza), `www4.ncsu.edu/~aiovchin/` (Alexey Ovchinnikov).

[1] The work was partially supported by the Russian Foundation for Basic Research, project no. 05-01-00671.

[2] This author was also partially supported by NSF Grant CCR-0096842.

[3] This author was also partially supported by NSERC Grant PDF-301108-2004.

[4] This author was also partially supported by NSERC Grant RGPIN *Algorithms and software for triangular decompositions of algebraic and differential systems.*

work are proven only for the **ordinary** case. We consider the following **two** bounding problems. The **first** problem is to bound the orders of all intermediate polynomials and the output of the Rosenfeld-Gröbner algorithm. In order to obtain such a bound in Proposition 10, we have modified this algorithm (see Algorithms 3 and 5) a little bit.

It would be good to have a bound that would tell us how many times we need to differentiate the original system in the beginning of the algorithm, so that the rest of the computation can be performed by a purely algebraic decomposition algorithm. Since for algebraic decomposition algorithms complexity estimates are known (see Szántó (1999)), such a bound would yield a complexity estimate for the differential decomposition as well. In this paper, however, we do not provide such a bound and, moreover, conjecture that it would have solved the Ritt problem (Ritt, 1950). We leave the discovery of such bound and/or the proof of this conjecture for future research.

Nevertheless, for the **second** type of the algorithms we are looking at in this paper we obtain such a bound. Namely, we can tell how many times one needs to differentiate elements of a *given characteristic set* of a characterizable differential ideal w.r.t. *one* differential ranking, in order to obtain a characteristic *decomposition* of this ideal w.r.t. *another* ranking. In other words, we give a bound for the conversion algorithm (Algorithm 8) for a characterizable ideal from one ranking to another (see Boulier (1999); Boulier et al. (2001); Golubitsky (2004) for other conversion algorithms applicable to prime differential ideals). We emphasize that the input ideal does not have to be characterizable w.r.t. the target ranking. We show how to obtain its new characteristic decomposition by first differentiating the input characteristic set and then applying only algebraic operations (i.e., a purely algebraic decomposition algorithm).

The paper is organized as follows. We give an introduction into differential algebra in Section 2. Then we describe the original Rosenfeld-Gröbner algorithm in Section 3. Section 4 is devoted to the bound on the orders of derivatives computed by a modified version of the Rosenfeld-Gröbner algorithm. After that, we show how to transform a characteristic set of a characterizable differential ideal into a characteristic decomposition of this ideal w.r.t. another differential ranking. We first do this for prime differential ideals (Section 5) and then treat the characterizable case in Section 6.

2. Definitions and notation

Differential algebra studies systems of polynomial partial differential equations from the algebraic point of view. The approach is based on the concept of differential ring introduced by Ritt. Recent tutorials on the constructive theory of differential ideals are presented in Boulier (2001, 2006); Hubert (2003); Sit (2002). A differential ring is a commutative ring with the unity endowed with a set of derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$, which commute pairwise. The case of $\Delta = \{\delta\}$ is called *ordinary*. If R is an ordinary differential ring and $y \in R$, we denote $\delta^k y$ by $y^{(k)}$.

Construct the multiplicative monoid $\Theta = \left\{ \delta_1^{k_1} \delta_2^{k_2} \cdots \delta_m^{k_m} \mid k_i \geqslant 0 \right\}$ of *derivative operators*. Let $Y = \{y_1, \ldots, y_n\}$ be a set whose elements are called *differential indeterminates*. The elements of the set $\Theta Y = \{\theta y \mid \theta \in \Theta,\ y \in Y\}$ are called *derivatives*. Derivative operators from Θ act on derivatives as $\theta_1(\theta_2 y_i) = (\theta_1\theta_2)y_i$ for all $\theta_1, \theta_2 \in \Theta$ and $1 \leqslant i \leqslant n$.

The ring of *differential polynomials* in differential indeterminates Y over a differential field $\mathbf{k}$ is a ring of commutative polynomials with coefficients in $\mathbf{k}$ in the infinite set of

variables ΘY (see Kolchin (1973); Kondratieva et al. (1999); Ritt (1950)). This ring is denoted $\mathbf{k}\{y_1, \ldots, y_n\}$ or $\mathbf{k}\{Y\}$. We consider the case of $\operatorname{char}\mathbf{k} = 0$ only. An ideal I in $\mathbf{k}\{Y\}$ is called *differential*, if for all $f \in I$ and $\delta \in \Delta$, $\delta f \in I$. We denote differential polynomials by $f, g, h, \ldots$ and use letters $I, J, \mathfrak{p}$ for ideals.

Let $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ be a set of differential polynomials. For the differential and radical differential ideal generated by F in $k\{y_1, \ldots, y_n\}$, we use notations $[F]$ and $\{F\}$, respectively.

We need the notion of reduction for algorithmic computations. First, we introduce a *ranking* on the set of derivatives. A ranking (Kolchin, 1973) is a total order $>$ on the set ΘY satisfying the following conditions for all $\theta \in \Theta$ and $u, v \in \Theta Y$:

(1) $\theta u \geqslant u$,

(2) $u \geqslant v \Longrightarrow \theta u \geqslant \theta v$.

Let u be a derivative, that is, $u = \theta y_j$ for a derivative operator

$$\theta = \delta_1^{k_1} \delta_2^{k_2} \cdots \delta_m^{k_m} \in \Theta$$

and $1 \leqslant j \leqslant n$. The *order* of u is defined as

$$\operatorname{ord} u = \operatorname{ord} \theta = k_1 + \ldots + k_m.$$

If f is a differential polynomial, $f \notin \mathbf{k}$, then $\operatorname{ord} f$ denotes the maximal order of derivatives appearing effectively in f.

A ranking $>$ is called *orderly* iff $\operatorname{ord} u > \operatorname{ord} v$ implies $u > v$ for all derivatives u and v. A ranking $>_{el}$ is called an *elimination* ranking iff $y_i >_{el} y_j$ implies $\theta_1 y_i >_{el} \theta_2 y_j$ for all $\theta_1, \theta_2 \in \Theta$.

Let a ranking $<$ be fixed. The derivative θy_j of the highest rank appearing in a differential polynomial $f \in \mathbf{k}\{y_1, \ldots, y_n\} \setminus \mathbf{k}$ is called the *leader* of f. We denote the leader by $\operatorname{ld} f$ or $\mathbf{u}_f$. The indeterminate y_j is called the *leading variable* of f and denoted by $\operatorname{lv} f$. Represent f as a univariate polynomial in $\mathbf{u}_f$:

$$f = \mathbf{i}_f \mathbf{u}_f^d + a_1 \mathbf{u}_f^{d-1} + \ldots + a_d.$$

The monomial $\mathbf{u}_f^d$ is called the *rank* of f and is denoted by $\operatorname{rk} f$. Extend the ranking relation on derivatives variables to ranks: $u_1^{d_1} > u_2^{d_2}$ iff either $u_1 > u_2$ or $u_1 = u_2$ and $d_1 > d_2$.

The polynomial $\mathbf{i}_f$ is called the *initial* of f. Apply any $\delta \in \Delta$ to f:

$$\delta f = \frac{\partial f}{\partial \mathbf{u}_f} \delta \mathbf{u}_f + \delta \mathbf{i}_f \mathbf{u}_f^d + \delta a_1 \mathbf{u}_f^{d-1} + \ldots + \delta a_d.$$

The leader of δf is $\delta \mathbf{u}_f$ and the initial of δf is called the *separant* of f, denoted $\mathbf{s}_f$. If $\theta \in \Theta \setminus \{1\}$, then θf is called a *proper derivative* of f. Note that the initial of any proper derivative of f is equal to $\mathbf{s}_f$.

We say that a differential polynomial f is *partially reduced* w.r.t. g iff no proper derivative of $\mathbf{u}_g$ appears in f. A differential polynomial f is *algebraically reduced* w.r.t. g iff $\deg_{\mathbf{u}_g} f < \deg_{\mathbf{u}_g} g$. A differential polynomial f is *reduced* w.r.t. a differential polynomial g iff f is partially and algebraically reduced w.r.t. g. Consider any subset $\mathbb{A} \subset \mathbf{k}\{y_1, \ldots, y_l\} \setminus \mathbf{k}$. We say that $\mathbb{A}$ is autoreduced (respectively, algebraically autoreduced) iff each element of $\mathbb{A}$ is reduced (respectively, algebraically reduced) w.r.t. all the others.

Every autoreduced set is finite (Kolchin, 1973, Chapter I, Section 9) (but an algebraically autoreduced set in a ring of differential polynomials may be infinite). For autoreduced sets we use capital letters $\mathbb{A}, \mathbb{B}, \mathbb{C}, \ldots$ and notation $\mathbb{A} = A_1, \ldots, A_p$ to specify the list of the elements of $\mathbb{A}$ arranged in order of increasing rank.

We denote the sets of initials and separants of elements of $\mathbb{A}$ by $\mathbf{i}_\mathbb{A}$ and $\mathbf{s}_\mathbb{A}$, respectively. Let $H_A = \mathbf{i}_\mathbb{A} \cup \mathbf{s}_\mathbb{A}$. Let S be a finite set of differential polynomials. Denote by S^∞ the multiplicative set containing 1 and generated by S. Let I be an ideal in a commutative ring R. The *saturated ideal* $I : S^\infty$ is defined as $\{a \in R \mid \exists s \in S^\infty : sa \in I\}$. If I is a differential ideal then $I : S^\infty$ is also a differential ideal (see Kolchin (1973)).

Consider two polynomials f and g in $\mathbf{k}\{y_1, \ldots, y_n\}$. Let I be the differential ideal generated by g. Applying a finite number of pseudo-divisions, one can compute a *differential partial remainder* f_1 and a *differential remainder* f_2 of f w.r.t. g such that there exist $s \in S_g^\infty$ and $h \in H_g^\infty$ satisfying $sf \equiv f_1$ and $hf \equiv f_2 \mod I$ with f_1 and f_2 partially reduced and reduced w.r.t. g, respectively (see Hubert (2000) for definitions and the algorithm for computing remainders). We denote by $\mathsf{d\text{-}rem}(f, \mathbb{A})$ the differential remainder of a polynomial f w.r.t. an autoreduced set $\mathbb{A}$.

Let $\mathbb{A} = A_1, \ldots, A_r$ and $\mathbb{B} = B_1, \ldots, B_s$ be (algebraically) autoreduced sets. We say that $\mathbb{A}$ has lower rank than $\mathbb{B}$ if

- there exists $k \leqslant r, s$ such that $\operatorname{rank} A_i = \operatorname{rank} B_i$ for $1 \leqslant i < k$, and $\operatorname{rank} A_k < \operatorname{rank} B_k$,
- or if $r > s$ and $\operatorname{rank} A_i = \operatorname{rank} B_i$ for $1 \leqslant i \leqslant s$.

We say that $\operatorname{rank} \mathbb{A} = \operatorname{rank} \mathbb{B}$ iff $r = s$ and $\operatorname{rank} A_i = \operatorname{rank} B_i$ for $1 \leqslant i \leqslant r$.

The following notion of a characteristic set in *Kolchin's sense* in characteristic zero is crucial in our further discussions. It was first introduced by Ritt for prime differential ideals, and then extended by Kolchin to arbitrary differential ideals.

Definition 1 *(Kolchin, 1973, page 82) An autoreduced subset of the lowest rank in a set $X \subset \mathbf{k}\{Y\}$ is called a characteristic set of X.*

We call these sets *Kolchin characteristic sets* to avoid confusion with other notions, e.g., in Hubert (2000, 2003) characteristic sets are used in Kolchin's sense and in some other senses. A characteristic set in Kolchin's sense exists for any set $X \subset \mathbf{k}\{Y\}$ due to the fact that every family of autoreduced sets contains one of the least rank (see Kolchin (1973)).

As it is mentioned in (Kolchin, 1973, Lemma 8, page 82), in the case of $\operatorname{char} k = 0$, a set $\mathbb{A}$ is a characteristic set of a proper differential ideal I iff each element of I reduces to zero w.r.t. $\mathbb{A}$. Moreover, the leaders and the correspondent degrees of these leaders of any two characteristic sets of I coincide.

Definition 2 *(Hubert, 2000, Definition 2.6) A differential ideal I in $\mathbf{k}\{y_1, \ldots, y_l\}$ is said to be characterizable if there exists a characteristic set $\mathbb{A}$ of I in Kolchin's sense such that $I = [\mathbb{A}] : H_\mathbb{A}^\infty$. We call any such characteristic set $\mathbb{A}$ a characterizing set of I.*

Characterizable ideals are radical (Hubert, 2000, Theorem 4.4).

3. Rosenfeld-Gröbner algorithm for the ordinary case

A system of ordinary differential equations and inequalities $\mathbb{A} = 0, H \neq 0$, where $\mathbb{A}, H \subset \mathbf{k}\{Y\}$, is called regular (see Boulier et al. (1995)), if A is autoreduced, H is partially reduced w.r.t. $\mathbb{A}$, and $H \supseteq H_\mathbb{A}$, where $H_\mathbb{A}$ is the set of initials and separants of elements of $\mathbb{A}$ (in the partial differential case it is also required that the set $\mathbb{A}$ is coherent, but in the ordinary case this condition holds for any autoreduced set $\mathbb{A}$). For a regular

system $\mathbb{A}, H$, the differential ideal $[\mathbb{A}] : H^\infty$ is also called regular. Every regular ideal is radical (see Boulier et al. (1995)), and, according to the Rosenfeld Lemma, $f \in [\mathbb{A}] : H^\infty$ if and only if the partial remainder of f w.r.t. $\mathbb{A}$ belongs to the algebraic ideal $(\mathbb{A}) : H^\infty$.

The Rosenfeld-Gröbner algorithm proposed in Boulier et al. (1995, 1997) computes a regular decomposition of a given radical differential ideal $\{F\}$, i.e., a representation

$$\{F\} = \bigcap_{i=1}^{k} [\mathbb{A}_i] : H_i^\infty,$$

where $[\mathbb{A}_i] : H_i^\infty$ are regular differential ideals.

We begin with the following version of the Rosenfeld-Gröbner algorithm. It is very similar to the original algorithm presented in Boulier et al. (1995, 1997), except for the fact that we are in the ordinary case and need not deal with coherence. We also note that some of the regular systems computed by the version of the algorithm presented here may correspond to unit ideals; this can be checked later on by means of Gröbner basis computations as in Boulier et al. (1995) or via polynomial GCD computations modulo regular chains as in Boulier and Lemaire (2000). Finally, we follow the suggestion given in (Hubert, 2003, Improvements, page 73): it is recommended to reduce the multiplicative set H of initials and separants. If it turns out that one of them reduces to zero, then the corresponding saturated component contains 1 and therefore need not be considered.

Given a set F of differential polynomials, the Rosenfeld-Gröbner algorithm at first computes a characteristic set $\mathbb{C}$ of F, i.e., an autoreduced subset of F of the least rank. It may happen that $\operatorname{lv}\mathbb{C} \subsetneq \operatorname{lv} F$ (for example, take $F = \{x + y, y\}$ w.r.t. a ranking such that $x > y$). In other words, inclusion $F_1 \subset F_2$ does not imply that for the corresponding characteristic sets $\mathbb{C}_1$ and $\mathbb{C}_2$, we have $\mathbb{C}_1 \subseteq \mathbb{C}_2$. We need the latter property, in order to obtain the bound, so we are going to relax the requirement that $\mathbb{C}$ is autoreduced.

A subset $\mathbb{C}$ of $\mathbf{k}\{Y\} \setminus \mathbf{k}$ is called a weak d-triangular set (Hubert, 2003, Definition 3.7), if the set of its leaders $\operatorname{ld}\mathbb{C}$ is autoreduced. In the ordinary case, $\mathbb{C}$ is a weak d-triangular set if and only if the leading differential indeterminates $\operatorname{lv} f$, $f \in \mathbb{C}$, are all distinct. For a polynomial f and a weak d-triangular set $\mathbb{C}$, the pseudo-remainder $\mathsf{d\text{-}rem}(f, \mathbb{C})$ is defined via (Hubert, 2003, Algorithm 3.13).

We will replace the reduction of F w.r.t. an autoreduced set in the Rosenfeld-Gröbner algorithm by that w.r.t. a weak d-triangular set. We note that the version of the algorithm presented in (Hubert, 2003, Section 6) (Algorithms 6.8, 6.10, and 6.11) also computes differential pseudo-remainders w.r.t. weak d-triangular sets. Since the output regular systems must be partially autoreduced, at the very end, partial autoreduction of the weak d-triangular set $\mathbb{C}$ via (Hubert, 2003, Algorithm 6.8) is carried out. Alternatively, one could perform partial autoreduction every time a weak d-triangular set is updated. In the following section, we show how to perform this autoreduction, as well as computation of differential pseudo-remainders, so that the inequality $M(F \cup H) \leqslant (n-1)!M(F_0 \cup H_0)$ is preserved (see formula (1) below).

4. Modified Rosenfeld-Gröbner algorithm

For a set of differential polynomials F, let $m_i(F)$ be the maximal order of the differential indeterminate $y_i \in Y$ occurring in F. If y_i does not occur in F, we set $m_i(F) = 0$.

Algorithm 1 Rosenfeld-Gröbner(F_0, H_0)

INPUT: *finite sets of differential polynomials* F_0, H_0 *and a differential ranking*

OUTPUT: *a finite set* T *of regular systems such that*

$$\{F_0\} : H_0^\infty = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^\infty$$

$T := \varnothing, \quad U := \{(F_0, H_0)\}$

while $U \neq \varnothing$ **do**

Take and remove any $(F, H) \in U$

$\mathbb{C} :=$ *characteristic set of* F

$\bar{F} :=$ d-rem$(F \setminus \mathbb{C}, \mathbb{C}) \setminus \{0\}$

$\bar{H} :=$ d-rem$(H, \mathbb{C}) \cup H_{\mathbb{C}}$

if $\bar{F} \cap \mathbf{k} = \varnothing$ **and** $0 \notin \bar{H}$ **then**

if $\bar{F} = \varnothing$ **then** $T := T \cup \{(\mathbb{C}, \bar{H})\}$

else $U := U \cup \{(\bar{F} \cup \mathbb{C}, \bar{H})\}$

end if

end if

$U := U \cup \{(F \cup \{h\}, H) \mid h \in H_{\mathbb{C}},\ h \notin \mathbf{k} \cup H\}$

end while

return T

Let

$$M(F) = \sum_{i=1}^{n} m_i(F). \tag{1}$$

We propose a modification of the Rosenfeld-Gröbner algorithm (see Algorithm 3 below), in which for every intermediate system $(F, \mathbb{C}, H) \in U$, the bound

$$M(F \cup \mathbb{C} \cup H) \leqslant (n-1)! M(F_0 \cup H_0) \tag{2}$$

holds, where $F_0 = 0, H_0 \neq 0$ is the input system of equations and inequalities corresponding to the radical differential ideal $\{F_0\} : H_0^\infty$.

In the formula (2) we have a multiple $(n-1)!$. If the number of variables is equal to 1 or 2 it disappears. In the case of $n = 2$ Ritt proved the Jacobi bound for $|F_0| = 2$ and empty H_0 by the direct computation and his result does not have any multiple either. Consider the intuition behind the case of $n = 3$ by looking at a particular example.

Example 3 *Let* $F_0 = x+y+z$, x' *with the elimination ranking* $x > y > z$. *Then* $m_x = 1$, $m_y = m_z = 0$ *and*

$$M(F_0) = 1 + 0 + 0 = 1.$$

In order to find a characteristic set of the prime differential ideal $[F_0]$ *we reduce* x' *w.r.t.* $x+y+z$ *and get* $y'+z'$. *The output consists of two polynomials:*

$$\mathbb{C} = y'+z', x+y+z.$$

We have: $m_x(\mathbb{C}) = 0$, $m_y(\mathbb{C}) = 1$, *and* $m_z(\mathbb{C}) = 1$. *Hence,*

$$M(\mathbb{C}) = 0+1+1 = 2 > 1.$$

But $(n-1)! = (3-1)! = 2! = 2$ *and* $2 \leqslant 2 \cdot 1$.

4.1. Algebraic computation of differential remainders

The Rosenfeld-Gröbner algorithm requires to compute differential pseudo-remainders $R = \mathsf{d\text{-}rem}(F \setminus \mathbb{C}, \mathbb{C})$. If the ranking on derivatives is not orderly, the orders of some (non-leading) derivatives may grow as a result of the differential pseudo-reduction, so that we may have $m_i(R) > m_i(F)$ for some $i \in \{1, \ldots, n\}$. To ensure a bound on $m_i(R)$, we construct a triangular set [5] $\mathbb{B}$, such that the computation of the differential pseudo-remainders $\mathsf{d\text{-}rem}(F, \mathbb{C})$ can be replaced by the computation of algebraic pseudo-remainders $\mathsf{algrem}(F, \mathbb{B})$, and, at the same time, $\mathbb{B}$ satisfies a bound on the orders of derivatives occurring in it. Moreover, $\mathbb{B}$ will contain a differentially triangular subset $\mathbb{B}^0$, which can be thought of as a result of autoreduction of $\mathbb{C}$.

Before we prove correctness and termination of Algorithm Differentiate&Autoreduce, let us discuss it informally. The triangular set $\mathbb{B}$ computed by the algorithm can be thought of as a result of an autoreduction of a *differential prolongation* of the input set $\mathbb{C} = \{C_1, \ldots, C_k\}$, i.e., of the set

$$\tilde{\mathbb{C}} = \{\delta^j C_i \mid 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i\}.$$

In particular, we have $\operatorname{rk}\mathbb{B} = \operatorname{rk}\tilde{\mathbb{C}}$, unless the autoreduction process cancels one of the initials, in which case we can show that $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} = (1)$.

However, if one wants to make this autoreduction completely algebraic (in order to control the growth of orders), one has to be careful, because in the above set $\tilde{\mathbb{C}}$ there may appear derivatives of some $\operatorname{ld} C_i$ of order higher than those that appear in $\operatorname{ld}\tilde{\mathbb{C}}$, which cannot be canceled by an algebraic reduction. For example, if $\mathbb{C} = \{y_1, y_2 + y_1'\}$, $m_1 = 1$, $m_2 = 2$, and the ranking is elimination with $y_1 < y_2$, then

$$\tilde{\mathbb{C}} = \{y_1, y_1', y_2 + y_1', y_2' + y_1'', y_2'' + y_1'''\},$$

and in the last two polynomials derivatives y_1'', y_1''' cannot be canceled by algebraic reduction w.r.t. y_1 and y_1'.

This problem is avoided by computing the elements of $\mathbb{B}$ in the order of increasing rank. If the polynomials are added to $\mathbb{B}$ in this order, one only needs to reduce each new polynomial f, which we are going to add to $\mathbb{B}$, w.r.t. the set $\delta\mathbb{B}$ of first-order derivatives of the elements of $\mathbb{B}$ and the set $\mathbb{B}^0$ with the same leaders as $\mathbb{C}$; this will guarantee that f is reduced w.r.t. $\mathbb{B}$.

The inclusions $\mathbb{B} \subset [\mathbb{B}^0] \subset [\mathbb{C}] \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty}$, $H_{\mathbb{B}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]$, and $H_{\mathbb{C}} \subset (H_{\mathbb{B}}^{\infty} + [\mathbb{B}]) : H_{\mathbb{B}}^{\infty}$ will allow us to replace reduction w.r.t. $\mathbb{C}$ (in the Rosenfeld-Gröbner algorithm) by that w.r.t. $\mathbb{B}$ without disturbing the saturated ideal. If m_i's are chosen as the maximal orders of derivatives of y_i's, $1 \leqslant i \leqslant k$, appearing in the set that is being reduced w.r.t. $\mathbb{C}$, then

[5] A set is called triangular if the leaders of its elements are distinct.

Algorithm 2 Differentiate&Autoreduce($\mathbb{C}, \{m_i\}$)

INPUT: *a weak d-triangular set* $\mathbb{C} = C_1, \dots, C_k$ *with* $\operatorname{ld}\mathbb{C} = y_1^{(d_1)}, \dots, y_k^{(d_k)}$, *and a set of non-negative integers* $\{m_i\}_{i=1}^k$, $m_i \geqslant m_i(\mathbb{C})$

OUTPUT: *set* $\mathbb{B} = \left\{ B_i^j \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i \right\}$ *satisfying*

$\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$

$\mathbb{B} \subset \left[\mathbb{B}^0\right] \subset [\mathbb{C}] \subset [\mathbb{B}] : H_{\mathbb{B}}^\infty$, *where* $\mathbb{B}^0 = \left\{ B_i^0 \;\middle|\; 1 \leqslant i \leqslant k \right\}$

$H_{\mathbb{B}} \subset H_{\mathbb{C}}^\infty + [\mathbb{C}], \quad H_{\mathbb{C}} \subset (H_{\mathbb{B}}^\infty + [\mathbb{B}]) : H_{\mathbb{B}}^\infty$

B_i^j *are reduced w.r.t.* $\mathbb{C} \setminus \{C_i\}$

$m_i(\mathbb{B}) \leqslant m_i$, $i = 1, \dots, k$

$m_i(\mathbb{B}) \leqslant m_i(\mathbb{C}) + \sum_{j=1}^k (m_j - d_j)$, $i = k+1, \dots, n$

or $\{1\}$, *if it is detected that* $[\mathbb{C}] : H_{\mathbb{C}}^\infty = (1)$

1 $\mathbb{D} := \mathbb{C}$, $\mathbb{B} := \varnothing$

2 **while** $\mathbb{D} \neq \varnothing$ **do**

3 *let* f *be the element of* $\mathbb{D}$ *of the least rank with* $\operatorname{ld} f = y_i^{(d)}$

4 $\bar{f} := \mathsf{algrem}\left(f, \left(\mathbb{B}^0 \cup \delta\mathbb{B}\right) \setminus \{f\}\right)$

5 **if** $\operatorname{rk}\bar{f} \neq \operatorname{rk} f$ **then return** $\{1\}$ **end if**

6 $\mathbb{D} := \mathbb{D} \setminus \{f\}$

7 **if** $d < m_i$ **then** $\mathbb{D} := \mathbb{D} \cup \left\{\delta\bar{f}\right\}$ **end if**

8 $\mathbb{B} := \mathbb{B} \cup \left\{\bar{f}\right\}$

9 **end while**

10 **return** $\mathbb{B}$

we can replace the differential reduction w.r.t. $\mathbb{C}$ by the algebraic reduction w.r.t. $\mathbb{B}$. The orders of derivatives of y_i's appearing in the remainder then will not exceed d_i for the leading y_i's (i.e., for $1 \leqslant i \leqslant k$). For the non-leading y_i's, the orders are bounded by the inequality

$$m_i(\mathbb{B}) \leqslant m_i(\mathbb{C}) + \sum_{j=1}^{k} (m_j - d_j), \quad i = k+1, \dots, n. \tag{3}$$

We will use the following two lemmas in the proof of correctness of Algorithm Differentiate&Autoreduce.

Lemma 4 *Let* $\mathbb{C}$ *be a weak d-triangular set in the ring of differential polynomials* $\mathbf{k}\{Y\}$ *with derivations* $\Delta = \{\delta_1, \dots, \delta_m\}$. *Assume that a ranking on the set of derivatives* ΘY *is fixed. Let* $f \in \mathbf{k}\{Y\}$ *be a differential polynomial with* $\operatorname{ld} f \notin \Theta \operatorname{ld}\mathbb{C}$, *and let* $f \to_{\mathbb{C}} g$. *Then*

- $\operatorname{rk} g < \operatorname{rk} f \;\Rightarrow\; \mathbf{i}_f \in [\mathbb{C}] : H_{\mathbb{C}}^\infty$
- $\operatorname{rk} g = \operatorname{rk} f \;\Rightarrow\; \exists\, h \in H_{\mathbb{C}}^\infty$ *such that* $h \cdot \mathbf{i}_f - \mathbf{i}_g \in [\mathbb{C}]$, $h \cdot \mathbf{s}_f - \mathbf{s}_g \in [\mathbb{C}]$.

Proof. Let $\operatorname{rk} f = u^d$, and let $\mathbb{A} = \{p \in \Theta\mathbb{C} \mid \operatorname{ld} p < u\}$. Then for every $p \in \mathbb{A}$, p and $\mathbf{i}_p$ are free of u.

Since $f \to_{\mathbb{C}} g$ and $u \notin \Theta \operatorname{ld} \mathbb{C}$, there exist polynomials $h \in \mathbf{i}_{\mathbb{A}}^{\infty}$, $A_1, \ldots, A_k \in \mathbb{A}$ and $\alpha_a, \ldots, \alpha_k \in \mathbf{k}\{Y\}$ such that

$$h \cdot f = g + \sum_{i=1}^{k} \alpha_i A_i. \tag{4}$$

The maximal degree of u present in (4) is equal to d. *Replace* every occurrence of u^d by a new variable v, and consider (4) as an equality between two polynomials in v, in which polynomials $h, A_1, \ldots, A_k$ are free of v. We have therefore:

$$h \cdot \frac{df}{dv} = \frac{dg}{dv} + \sum_{i=1}^{k} \frac{d\alpha_i}{dv} A_i.$$

It remains to notice that $\frac{df}{dv} = \mathbf{i}_f$ and

$$\frac{dg}{dv} = \begin{cases} 0, & \operatorname{rk} g < \operatorname{rk} f \\ \mathbf{i}_g, & \operatorname{rk} g = \operatorname{rk} f \end{cases},$$

hence we obtain

- $\operatorname{rk} g < \operatorname{rk} f \;\Rightarrow\; \mathbf{i}_f \in (\mathbb{A}) : \mathbf{i}_{\mathbb{A}}^{\infty} \subset [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$.
- $\operatorname{rk} g = \operatorname{rk} f \;\Rightarrow\; h \cdot \mathbf{i}_f - \mathbf{i}_g \in (\mathbb{A}) \subset [\mathbb{C}]$, where $h \in \mathbf{i}_{\mathbb{A}}^{\infty} \subset H_{\mathbb{C}}^{\infty}$.

Consider now (4) as an equality between two polynomials in u, in which $h, A_1, \ldots, A_k$ are free of u. We have therefore:

$$h \cdot \frac{df}{du} = \frac{dg}{du} + \sum_{i=1}^{k} \frac{d\alpha_i}{du} A_i.$$

It remains to notice that $\frac{df}{du} = \mathbf{s}_f$ and, if $\operatorname{rk} g = \operatorname{rk} f$, $\frac{dg}{du} = \mathbf{s}_g$, hence $h \cdot \mathbf{s}_f - \mathbf{s}_g \in (\mathbb{A}) \subset [\mathbb{C}]$, where $h \in \mathbf{i}_{\mathbb{A}}^{\infty} \subset H_{\mathbb{C}}^{\infty}$. □

Remark 5 *The above lemma also holds when the set of derivations Δ is empty, in which case $\mathbf{k}\{Y\} = \mathbf{k}[Y]$ is a ring of algebraic polynomials, $\mathbb{C} \subset \mathbf{k}[Y]$ is a triangular set, $\to_{\mathbb{C}}$ is the algebraic pseudo-reduction relation w.r.t. $\mathbb{C}$, and $[\mathbb{C}] = (\mathbb{C})$ is an ideal in $\mathbf{k}[Y]$.*

Lemma 6 *(Hubert, 2003, Lemma 6.9) Let H and K be two sets of differential polynomials, and let I be a differential ideal. If $K \subset (H^{\infty} + I) : H^{\infty}$, then $I : H^{\infty} = I : (H \cup K)^{\infty}$.*

Proof. The proof of this statement is omitted in Hubert (2003), so, for the sake of completeness, we provide it here.

Clearly, $I : H^{\infty} \subseteq I : (H \cup K)^{\infty}$. To prove the inverse inclusion, take any $f \in I : (H \cup K)^{\infty}$. Then, by definition, there exist $h \in H^{\infty}$ and $k \in K^{\infty}$ such that $fhk \in I$.

Since $K \subset (H^{\infty} + I) : H^{\infty}$, there exist $h_1, h_2 \in H^{\infty}$ such that $kh_1 - h_2 \in I$. The fact that $fhk \in I$ implies that $fhkh_1 \in I$, whence

$$fhkh_1 - fh(kh_1 - h_2) = fhh_2 \in I,$$

i.e., $f \in I : H^{\infty}$. □

Proposition 7 *Algorithm* Differentiate&Autoreduce *is correct and terminates.*

Proof. We show that the following invariants hold for the **while**-loop in Algorithm 2:

(I1) $\mathbb{B} = \left\{ B_i^j \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant j_i \right\}$, where $-1 \leqslant j_i \leqslant m_i - d_i$.

(I2) $\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$, $(1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant j_i)$

(I3) $m_t\left(B_i^j\right) \leqslant d_t$, $(1 \leqslant i \neq t \leqslant k,\ 0 \leqslant j \leqslant j_i)$

(I4) $\mathbb{B} \subset \left[\mathbb{B}^0\right]$, where $\mathbb{B}^0 = \left\{ B_i^0 \mid 1 \leqslant i \leqslant k,\ j_i \geq 0 \right\}$

(I5) $\mathbb{D} = \left\{ D_i \mid 1 \leqslant i \leqslant k,\ j_i < m_i - d_i \right\} \subset \mathbb{C} \cup \delta\mathbb{B}$

(I6) $\operatorname{rk} D_i = \operatorname{rk} C_i^{(j_i+1)}$ $(1 \leqslant i \leqslant k,\ j_i < m_i - d_i)$

(I7) $m_i(\mathbb{D}) \leqslant m_i + 1$ $(1 \leqslant i \leqslant k,\ j_i < m_i - d_i)$

(I8) $\mathbb{B} \cup \mathbb{D} \subset [\mathbb{C}]$

(I9) $\mathbb{C} \setminus \mathbb{D} \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty}$

(I10) $H_{\mathbb{B} \cup \mathbb{D}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]$

(I11) $H_{\mathbb{C} \setminus \mathbb{D}} \subset (H_{\mathbb{B}}^{\infty} + [\mathbb{B}]) : H_{\mathbb{B}}^{\infty}$

The invariants I1–I11 hold initially, when $\mathbb{D} = \mathbb{C}$ and $\mathbb{B} = \varnothing$. Assuming that the invariants hold at the beginning of an iteration of the **while**-loop, we will show that they also hold at the end of this iteration.

Let f be the element of $\mathbb{D}$ of the least rank computed in line 3, and let $y_i^{(d)} = \operatorname{ld} f$. Then I5 implies that

$$j_i < m_i - d_i, \tag{5}$$

and I6 yields

$$\operatorname{rk} f = \operatorname{rk} C_i^{(j_i+1)} \tag{6}$$

Also, due to I8, we have

$$f \in [\mathbb{C}], \tag{7}$$

and due to I10

$$H_f \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]. \tag{8}$$

We will show that

$$m_t(f) \leqslant d_t + j_t + 1 \quad \forall\, t \in \{1, \ldots, k\} \setminus \{i\}. \tag{9}$$

Indeed, invariant I1 says that $j_t \leqslant m_t - d_t$, hence two cases are possible:

- Case 1: $j_t < m_t - d_t$. According to I5 and I6, there exists $D_t \in \mathbb{D}$ with $\operatorname{rk} D_t = \operatorname{rk} C_t^{(j_t+1)}$. Since f is an element of $\mathbb{D}$ of the least rank, $\operatorname{rk} f \leqslant \operatorname{rk} D_t$, hence $m_t(f) \leqslant d_t + j_t + 1$.
- Case 2: $j_t = m_t - d_t$. In this case, invariant I7 implies that $m_t(f) \leqslant m_t + 1 = d_t + j_t + 1$. Since $\bar{f} = \mathsf{algrem}\left(f, (\delta\mathbb{B}) \setminus \{f\}\right)$, we have:

$$f \in \left[\mathbb{B} \cup \left\{\bar{f}\right\}\right] : H_{\mathbb{B}}^{\infty}. \tag{10}$$

Moreover, if $\operatorname{rk} f = \operatorname{rk} C_i^{(j)}$, $j > 0$, then $f \notin \mathbb{C}$, since $\mathbb{C}$ is a weak d-triangular set. Thus, due to I5, $f \in \delta\mathbb{B}$. Taking into account I4, we obtain that

$$\operatorname{rk} f = \operatorname{rk} C_i^{(j)},\ j > 0 \quad \Rightarrow \quad \bar{f} \in \left[\mathbb{B}^0\right]. \tag{11}$$

Assuming that $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} \neq (1)$, let us demonstrate that

$$\operatorname{rk} \bar{f} = \operatorname{rk} f. \tag{12}$$

Let us show first that $\operatorname{ld} f \notin \operatorname{ld}(\delta\mathbb{B} \setminus \{f\})$. Indeed, according to I1 and I2,

$$\operatorname{ld} \mathbb{B} = \left\{ \operatorname{ld} C_i^{(j)} \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant j_i \right\}. \tag{13}$$

Thus, if $\operatorname{ld} f \in \operatorname{ld} \delta\mathbb{B}$, then $\operatorname{ld} f \notin \operatorname{ld} \mathbb{C}$, whence $f \notin \mathbb{C}$. Recall that $f \in \delta\mathbb{B}$.

Suppose that $\operatorname{rk} \bar{f} < \operatorname{rk} f$. Then by Lemma 4 and Remark 5, $\mathbf{i}_f \in (\mathbb{B}) : H_{\mathbb{B}}^{\infty}$. According to I8, $\mathbb{B} \subset [\mathbb{C}]$, hence

$$(\mathbb{B}) : H_{\mathbb{B}}^{\infty} \subset [\mathbb{C}] : H_{\mathbb{B}}^{\infty} \subset [\mathbb{C}] : (H_{\mathbb{B}} \cup H_{\mathbb{C}})^{\infty}.$$

According to I10, $H_{\mathbb{B}} \subset H_C^{\infty} + [\mathbb{C}]$. Thus, Lemma 6 with $H = H_{\mathbb{C}}$, $K = H_{\mathbb{B}}$, and $I = [\mathbb{C}]$ yields $[\mathbb{C}] : (H_{\mathbb{B}} \cup H_{\mathbb{C}})^{\infty} = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$, whence $(\mathbb{B}) : H_{\mathbb{B}}^{\infty} \subset [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$. In particular, this implies that $\mathbf{i}_f \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$, which together with (8) leads to a contradiction with the assumption that $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} \neq (1)$. Thus, $\operatorname{rk} \bar{f} = \operatorname{rk} f$. Taking into account (6), we obtain

$$\operatorname{rk} \bar{f} = \operatorname{rk} C_i^{(j_i+1)} \tag{14}$$

Moreover, Lemma 4 also states that

$$H_{\bar{f}} \subset H_f \cdot H_{\mathbb{B}}^{\infty} + (\mathbb{B}), \tag{15}$$

as well as

$$H_f \subset \left(H_{\bar{f}} \cdot H_{\mathbb{B}}^{\infty} + (\mathbb{B})\right) : H_{\mathbb{B}}^{\infty}. \tag{16}$$

Inclusion (15) together with I8 and I10 implies that

$$H_{\bar{f}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]. \tag{17}$$

Let $t \in \{1, \ldots, k\} \setminus \{i\}$. Invariants I2 and I3 imply that $m_t(\delta\mathbb{B}) \leqslant d_t + j_t + 1$. Combining this inequality with (9), we obtain

$$m_t\left(\bar{f}\right) \leqslant d_t + j_t + 1.$$

Now, since $\bar{f}$ is algebraically reduced w.r.t. $\delta\mathbb{B}$, whose leaders are given by (13), we have

$$m_t\left(\bar{f}\right) \leqslant d_t \quad \forall\, t \in \{1, \ldots, k\} \setminus \{i\}. \tag{18}$$

Finally, (7) and I8 imply that

$$\bar{f} \in [\mathbb{C}]. \tag{19}$$

Now, using statements (5–19), we are ready to show that invariants I1–I11 hold at the end of the **while**-loop. We have:

- Due to (5,14) and the assignment performed in line 8 of the algorithm, I1 and I2 hold.
- Due to (18), I3 holds.
- If $\operatorname{rk} f = \operatorname{rk} C_i$, then $B_i^0 = \bar{f}$ due to line 8 and (12). If $\operatorname{rk} f = \operatorname{rk} C_i^{(j)}$, $j > 0$, then by (11) $\bar{f} \in [\mathbb{B}^0]$. In both cases, I4 holds.
- Due to lines 6, 7, and 8, I5 holds.
- Due to (14), I6 holds.
- Due to (14) and (18), I7 holds.
- Due to (19) and former I8, I8 holds.
- Due to (17) and former I10, I10 holds.
- Due to (10), I9 holds.
- Due to (16), I11 holds.

The algorithm can terminate either as a result of the **return**-statement in line 5, or because the **while**-loop terminates. We have shown that the condition of the **if**-statement in line 5, namely $\operatorname{rk} \bar{f} \neq \operatorname{rk} f$, can be satisfied only if $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} = (1)$, in which case the algorithm correctly returns $\{1\}$.

Now assume that condition of the **if**-statement in line 5 is never satisfied. Then, at every iteration, exactly one of the indices j_i increases, due to (14) and line 8. Since

initially $\mathbb{B} = \varnothing$, i.e., $j_i = -1$, $1 \leqslant i \leqslant k$, and due to the fact that $j_i \leqslant m_i - d_i$, $1 \leqslant i \leqslant k$ (invariant I1), the number of iterations of the **while**-loop is equal to

$$\sum_{j=1}^{k} (m_j - d_j). \tag{20}$$

Therefore, the algorithm terminates.

Invariants I1–I11 also imply the correctness of the output $\mathbb{B}$. Namely, at the exit from the **while**-loop due to $\mathbb{D} = \varnothing$ we have:

- I1 and I5 imply that $j_i = m_i - d_i$, $1 \leqslant i \leqslant k$.
- Hence, I1 becomes $\mathbb{B} = \left\{ B_i^j \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i \right\}$.
- According to I2, $\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$.
- According to I4, I8, and I9, we have $\mathbb{B} \subset [\mathbb{B}^0] \subset [\mathbb{C}]$ and $\mathbb{C} \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty}$.
- According to I10 and I11, we have $H_{\mathbb{B}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]$ and $H_{\mathbb{B}}^{\infty} H_{\mathbb{C}} \subset H_{\mathbb{B}}^{\infty} + [\mathbb{B}]$.
- Due to I2 and I3, B_i^j are reduced w.r.t. $\mathbb{C} \setminus \{C_i\}$.
- At each iteration, every polynomial in $\mathbb{B} \cup \mathbb{D}$ is differentiated at most once (in line 4 or 7). Therefore, with each iteration, $m_i(\mathbb{B} \cup \mathbb{D})$, $i = k+1, \ldots, n$, can increase maximum by 1. Since the number of iterations is given by (20), at the exit from the **while**-loop we have

$$m_i(\mathbb{B}) \leqslant m_i(\mathbb{C}) + \sum_{j=1}^{k} (m_j - d_j), \quad i = k+1, \ldots, n.$$

This concludes the proof of correctness. □

4.2. Final algorithm and proof of the bound

We are ready to present a modified version of the Rosenfeld-Gröbner algorithm that satisfies the bound. The only place where the orders of derivatives may grow is the pseudoreduction w.r.t. an autoreduced set $\mathbb{C}$. Of course, only the orders of non-leading differential indeterminates may grow, while the orders of the leading ones decrease as a result of reduction (or stay the same if the reduction turns out to be algebraic, but then the orders of non-leading indeterminates do not grow either).

By associating different weights with leading and non-leading indeterminates, we will achieve that the weighted sum of their orders does not increase as a result of reduction. These weights come from the bound in the algorithm Differentiate&Autoreduce. If the set of leading indeterminates changes, so do the weights. However, if we estimate in advance the number of times the set of leading indeterminates can change throughout the algorithm, we can still obtain an overall bound on the orders.

For the original Rosenfeld-Gröbner algorithm, it is not that easy to carry out such an estimate, because some indeterminates may disappear and reappear again among the leading indeterminates of the characteristic set $\mathbb{C}$. For example,

Example 8 *Let $F = \{y + z,\ x,\ x^2 + z\}$, with the elimination ranking $x > y > z$.*

- *We choose its characteristic set as $\mathbb{C} := \{y + z,\ x\}$.*
- *The leading variables of $\mathbb{C}$ are $\{y, x\}$.*
- *We put $\bar{F} := \mathsf{d\text{-}rem}(F \setminus \mathbb{C}, \mathbb{C}) = \{z\}$.*
- *$F_{\text{new}} := \bar{F} \cup \mathbb{C} = \{z,\ y + z,\ x\}$.*

- *As radical differential ideals:*

$$\{y+z, x, x^2+z\} = [z, y+z, x] : 1^\infty \cap \{y+z, x, x^2+z, 1\}.$$

- *The new* $\mathbb{C} = \{z,\ x\}$ *is computed from* F_{new} *and the leading variables have changed!*
- ...

- *Finally,*

$$\{y+z, x, x^2+z\} = [z, y, x] : 1^\infty = [z, y, x]$$

and we see that the leaders y *and* x *have come back.*

Example 9 *Let* $F = \{zy,\ x,\ x^2+z\}$*, with the elimination ranking* $x > y > z$*.*

- *We choose its characteristic set as* $\mathbb{C} := \{zy,\ x\}$*.*
- *The leading variables of* $\mathbb{C}$ *are* $\{y, x\}$*.*
- *We put* $\bar{F} :=$ d-rem$(F \setminus \mathbb{C}, \mathbb{C}) = \{z\}$*.*
- $F_{\text{new}} := \bar{F} \cup \mathbb{C} = \{z,\ zy,\ x\}$*.*
- *As radical differential ideals:*

$$\{zy, x, x^2+z\} = [z, zy, x] : z^\infty \cap \{zy, x, x^2+z, z\}.$$

- *The new* $\mathbb{C} = \{z, x\}$ *is computed from* F_{new} *and the leading variables have also changed!*
- *But the first component is trivial:* $1 \in [z, zy, x] : z^\infty$*.*

The first situation can be remedied by properly relaxing the requirement that $\mathbb{C}$ is autoreduced, while the second one can detected, after which further computations in this branch of the Rosenfeld-Gröbner algorithm are not necessary. As a result, we obtain an algorithm, in which, as long as an indeterminate appears among the leading indeterminates of the set $\mathbb{C}$, w.r.t. which we reduce, it will stay there until the end.

As mentioned above, we are going to replace the computation of the characteristic set by that of a weak d-triangular subset. It is tempting to simply compute a weak d-triangular subset of the least rank, since this computation is inexpensive and it would give us the desired property that the leading indeterminates do not disappear. However, the termination of the algorithm is not guaranteed then. For example, take the system $F = \{x, xy\}$ in $\mathbf{k}\{x, y\}$, and let $x < y$. The weak d-triangular subset of F of the least rank is F itself. Thus, we obtain a component $\{x, xy\} : x^\infty = (1)$ and another component $\{x, xy, \mathbf{i}_{xy}\}$. However, $\mathbf{i}_{xy} = x$, hence we arrive at the same set F that was given in the input, and the algorithm runs forever.

The reason for the above behavior is that the initials of a weak d-triangular set $\mathbb{C}$, as opposed to an autoreduced set, need not be reduced w.r.t. $\mathbb{C}$. Thus by adding these initials we do not necessarily decrease the rank. The solution comes from the idea of (Boulier et al., 1997, Section 5), (Hubert, 2003, Algorithm 6.11), and (Hubert, 2004, Algorithm 4.1) to construct the weak d-triangular set $\mathbb{C}$ gradually, so that each next polynomial f to be added to $\mathbb{C}$ is reduced w.r.t. $\mathbb{C}$ (thus, we can also safely add the initial and separant of f and guarantee that the rank decreases). In order to be able to construct the set $\mathbb{C}$ gradually, similarly to Hubert (2003), we store it as a separate component of the triples $(F, \mathbb{C}, H) \in U$.

The last modification that we are going to do is the replacement of the differential pseudo-reduction w.r.t. $\mathbb{C}$ by the algebraic pseudo-reduction w.r.t. $\mathbb{B}$, which is computed from $\mathbb{C}$ by Algorithm Differentiate&Autoreduce. As a result, we obtain Algorithm RG-Bound.

Algorithm 3 RGBound(F_0, H_0)

INPUT: *finite sets of differential polynomials* $F_0 \neq \varnothing$ *and* H_0, *and a differential ranking*

OUTPUT: *a finite set* T *of regular systems such that*

$$\{F_0\} : H_0^\infty = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^\infty \quad \textit{and}$$

$$M(\mathbb{A} \cup H) \leqslant (n-1)!M(F_0 \cup H_0) \textit{ for } (\mathbb{A}, H) \in T.$$

$T := \varnothing, \quad U := \{(F_0, \varnothing, H_0)\}$
while $U \neq \varnothing$ **do**
  Take and remove any $(F, \mathbb{C}, H) \in U$
  $f :=$ *an element of* F *of the least rank*
  $D := \{C \in \mathbb{C} \mid \operatorname{lv} C = \operatorname{lv} f\}$
  $G := F \cup D \setminus \{f\}$
  $\bar{\mathbb{C}} := \mathbb{C} \setminus D \cup \{f\}$
  $\mathbb{B} :=$Differentiate&Autoreduce $\left(\bar{\mathbb{C}}, \left\{m_y(G \cup \bar{\mathbb{C}} \cup H) \mid y \in \operatorname{lv} \bar{\mathbb{C}}\right\}\right)$
  if $\mathbb{B} \neq \{1\}$ **then**
    $\bar{F} :=$ algrem$(G, \mathbb{B}) \setminus \{0\}$
    $\bar{H} :=$ algrem$(H, \mathbb{B}) \cup H_{\mathbb{B}}$
    if $\bar{F} \cap \mathbf{k} = \varnothing$ **and** $0 \notin \bar{H}$ **then**
      if $\bar{F} = \varnothing$ **then** $T := T \cup \{(\mathbb{B}^0, \bar{H})\}$
        else $U := U \cup \{(\bar{F}, \mathbb{B}^0, \bar{H})\}$
      end if
    end if
  end if
  if $\mathbf{s}_f \notin \mathbf{k}$ **then**
    $U := U \cup \{(F \cup \{\mathbf{s}_f\}, \mathbb{C}, H)\}$
    if $\mathbf{i}_f \notin \mathbf{k}$ **then** $U := U \cup \{(F \cup \{\mathbf{i}_f\}, \mathbb{C}, H)\}$ **end if**
  end if
end while
return T

In the proof of the bound, a key role is played by the quantity $M_Z(F)$, which is defined for a finite set F of differential polynomials and a proper subset $Z \subsetneq Y$. Assume that $|Z| = k < n$. As before, for a differential indeterminate $y \in Y$, $m_y(F)$ denotes the highest order of a derivative of y occurring in F, or zero, if y does not occur in F. Then

$$M_Z(F) := (n-k)\sum_{y\in Z} m_y(F) + \sum_{y\in Y\setminus Z} m_y(F).$$

We also recall the notation

$$M(F) = \sum_{y\in Y} m_y(F).$$

Proposition 10 *Algorithm* RGBound *is correct and terminates*

Proof. We prove the following invariants of the **while**-loop:

- (I1) $\{F_0\} : H_0^\infty = \bigcap_{(F,\mathbb{C},H)\in U}\{F\cup\mathbb{C}\} : H^\infty \cap \bigcap_{(\mathbb{A},H)\in T}[\mathbb{A}] : H^\infty$
- For all $(F, \mathbb{C}, H) \in U$,
  - (I2) $\mathbb{C}$ is d-triangular,
  - (I3) $F \neq \varnothing$ is reduced w.r.t. $\mathbb{C}$
  - (I4) $H_\mathbb{C} \subset H$,
  - (I5) Let $l = |\operatorname{lv}\mathbb{C}|$. Then, if $l < n$,

$$M_{\operatorname{lv}\mathbb{C}}(F\cup\mathbb{C}\cup H) \leqslant (n-1)\ldots(n-l)\cdot M(F_0\cup H_0),$$

otherwise

$$M(F\cup\mathbb{C}\cup H) \leqslant (n-1)!\cdot M(F_0\cup H_0).$$

The invariants hold for the initial triple $(F_0, \varnothing, H_0)$. Assuming that they hold at the beginning of an iteration of the **while** loop, we will show that the invariants also take place at the end of the iteration.

Let $(F, \mathbb{C}, H)$ be the triple taken and removed from U. Since $F \neq \varnothing$, we can compute an element $f \in F$ of the least rank. Then f, as an element of F, is reduced w.r.t. $\mathbb{C}$. Applying (Hubert, 2003, Proposition 6.6), we have

$$\{F\cup\mathbb{C}\} : H^\infty = \{F\cup\mathbb{C}\} : (H\cup H_f)^\infty \cap \{F\cup\{\mathbf{i}_f\}\cup\mathbb{C}\} : H^\infty \cap \{F\cup\{\mathbf{s}_f\}\cup\mathbb{C}\} : H^\infty.$$

We note that, since $\operatorname{rk}\mathbf{i}_f < \operatorname{rk} f$ and $\operatorname{rk}\mathbf{s}_f < \operatorname{rk} f$, polynomials $\mathbf{i}_f$ and $\mathbf{s}_f$ are, respectively, the elements of $F\cup\{\mathbf{i}_f\}$ and $F\cup\{\mathbf{s}_f\}$ of the least rank (and, to repeat, their ranks are less than the rank of the least element of F). Moreover, since in the last two triples $(F\cup\{\mathbf{i}_f\},\mathbb{C},H), (F\cup\{\mathbf{s}_f\},\mathbb{C},H)$ only the first component has changed, invariants I2–I5 are preserved for them. For the proof of invariant I1, it remains to show that

$$\{F\cup\mathbb{C}\} : (H\cup H_f)^\infty = \begin{cases} \left[\mathbb{B}^0\right] : \bar{H}^\infty, & \bar{F} = \varnothing \\ \left\{\bar{F}\cup\mathbb{B}^0\right\} : \bar{H}^\infty, & \text{otherwise.} \end{cases} \tag{21}$$

Given that $\mathbb{C}$ is d-triangular, the three assignments following the computation of f ensure that $\bar{\mathbb{C}}$ is a weak d-triangular set of rank strictly less than $\mathbb{C}$, because the polynomial f is reduced w.r.t. $\mathbb{C}$ and we throw away (from $\mathbb{C}$) all its elements with leading variables "in conflict" with the one of f. We note that

$$G\cup\bar{\mathbb{C}} = (F\cup\mathbb{D}\setminus\{f\})\cup(\mathbb{C}\setminus\mathbb{D})\cup\{f\} = F\cup\mathbb{C}.$$

Since $H_{\mathbb{C}} \subset H$, we also have $H \cup H_f = H \cup H_{\bar{\mathbb{C}}}$. Therefore,

$$\{F \cup \mathbb{C}\} : (H \cup H_f)^\infty = \left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}})^\infty . \tag{22}$$

Next, we use the properties of the set $\mathbb{B}$ ensured by Algorithm Differentiate&Autoreduce. Since $H_{\mathbb{B}} \subset H_{\bar{\mathbb{C}}}^\infty + \left[\bar{\mathbb{C}}\right]$, applying Lemma 6 with $K = H_{\mathbb{B}}$, we obtain

$$\left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}})^\infty = \left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty . \tag{23}$$

The inclusions $\mathbb{B} \subset \left[\bar{\mathbb{C}}\right]$ and $\bar{\mathbb{C}} \subset [\mathbb{B}] : H_{\mathbb{B}}^\infty$ imply that

$$\left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty = \{G \cup \mathbb{B}\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty . \tag{24}$$

Using the fact that $H_{\bar{\mathbb{C}}} \subset (H_{\mathbb{B}}^\infty + [\mathbb{B}]) : H_{\mathbb{B}}^\infty$ (see Algorithm 2) and applying Lemma 6 with $K = H_{\bar{\mathbb{C}}}$, we get

$$\{G \cup \mathbb{B}\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty = \{G \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty. \tag{25}$$

It follows from the definition of the algebraic pseudo-remainder (algrem) that

$$\{G \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty = \{\bar{F} \cup \mathbb{B}\} : \bar{H}^\infty. \tag{26}$$

Indeed, $\{G \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty = \{\bar{F} \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty$. Take now any $f \in \left\{\bar{F} \cup \mathbb{B}\right\} : (H \cup H_{\mathbb{B}})^\infty$. There exists $h \in (H \cup H_{\mathbb{B}})^\infty$ such that $h \cdot f \in \left\{\bar{F} \cup \mathbb{B}\right\}$. If $\bar{h}$ is a remainder of h w.r.t. $\mathbb{B}$ then there exists $h' \in H_{\mathbb{B}}^\infty$ with $h'h - \bar{h} \in (\mathbb{B})$. Hence,

$$\bar{h}f \in \left\{\bar{F} \cup \mathbb{B}\right\}$$

and

$$f \in \left\{\bar{F} \cup \mathbb{B}\right\} : \bar{H}^\infty.$$

The reverse inclusion is done in a similar way. Since $\mathbb{B} \subset \left[\mathbb{B}^0\right]$, we obtain that $\left\{\bar{F} \cup \mathbb{B}\right\} : \bar{H}^\infty = \left\{\bar{F} \cup \mathbb{B}^0\right\} : \bar{H}^\infty$.

The set $\mathbb{B}^0$ is d-triangular, its rank is equal to that of $\bar{\mathbb{C}}$, set $\bar{H}$ is partially reduced w.r.t. $\mathbb{B}^0$ and contains $H_{\mathbb{B}}^0$, and $\bar{F}$ is reduced w.r.t. $\mathbb{B}^0$. Moreover, if $\bar{F} = \varnothing$, we obtain the regular system $\left(\mathbb{B}^0, \bar{H}\right)$, which corresponds to the radical differential ideal $\left[\mathbb{B}^0\right] : \bar{H}^\infty = \left\{\bar{F} \cup \mathbb{B}^0\right\} : H_{\mathbb{B}}^\infty$. Thus, we have proved (21) and also have demonstrated that invariants I2–I4 hold for the triple $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$.

Termination of the algorithm is proved as follows. At each iteration of the **while**-loop, the triple $(F, \mathbb{C}, H) \in U$ is replaced by at most three triples $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$, $(F \cup \{\mathbf{i}_f\}, \mathbb{C}, H)$, and $(F \cup \{\mathbf{s}_f\}, \mathbb{C}, H)$. We have shown that in the first triple we have $\operatorname{rk} \mathbb{B}^0 < \operatorname{rk} \mathbb{C}$; in the last two triples the second component $\mathbb{C}$ remains the same, but the elements of the least rank of $F \cup \{\mathbf{i}_f\}$ and $F \cup \{\mathbf{s}_f\}$ are strictly less than the element of F of the least rank. That is, for each triple replacing $(F, \mathbb{C}, H)$, either the rank of the second component is lower, or it is the same, but the rank of the minimal element of the first component is lower. Therefore, all triples computed by the algorithm can be arranged in a ternary tree, in which $(F_0, \varnothing, H_0)$ is the root, and every path starting from the root is finite. This implies that the entire tree is finite, whence the algorithm terminates.

Finally, we show that invariant I5 holds for the triple $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$. We assume that $|\operatorname{lv} \mathbb{C}| = l$. Two cases are possible:

(1) $\operatorname{lv} f \in \operatorname{lv} \mathbb{C}$. Then $\operatorname{lv} \bar{\mathbb{C}} = \operatorname{lv} \mathbb{C}$ and for any finite set of polynomials K, if $l < n$, we have

$$M_{\operatorname{lv} \bar{\mathbb{C}}}(K) = M_{\operatorname{lv} \mathbb{C}}(K). \tag{27}$$

(2) $\operatorname{lv} f \notin \operatorname{lv} \mathbb{C}$. Then $\operatorname{lv} \bar{\mathbb{C}} = \operatorname{lv} \mathbb{C} \cup \{\operatorname{lv} f\}$ and $|\operatorname{lv} \bar{\mathbb{C}}| = l + 1$. If $l + 1 < n$, we observe that

$$
\begin{aligned}
&M_{\operatorname{lv} \bar{\mathbb{C}}}(K) = \\
&= (n-l-1) \sum_{y \in \operatorname{lv} \bar{\mathbb{C}}} m_y(K) + \sum_{y \notin \operatorname{lv} \bar{\mathbb{C}}} m_y(K) = \\
&= (n-l-1) \sum_{y \in \operatorname{lv} \mathbb{C}} m_y(K) + (n-l-1) \cdot m_{\operatorname{lv} f}(K) + \sum_{y \notin \operatorname{lv} \bar{\mathbb{C}}} m_y(K) = \\
&= (n-l-1) \sum_{y \in \operatorname{lv} \mathbb{C}} m_y(K) + (n-l-2) \cdot m_{\operatorname{lv} f}(K) + \\
&\quad + (m_{\operatorname{lv} f}(K) + \sum_{y \notin \operatorname{lv} \bar{\mathbb{C}}} m_y(K)) = \\
&= (n-l-1) \sum_{y \in \operatorname{lv} \mathbb{C}} m_y(K) + \sum_{y \notin \operatorname{lv} \mathbb{C}} m_y(K) + (n-l-2) \cdot m_{\operatorname{lv} f}(K) \leqslant \\
&\leqslant (n-l) \sum_{y \in \operatorname{lv} \mathbb{C}} m_y(K) + \sum_{y \notin \operatorname{lv} \mathbb{C}} m_y(K) + (n-l-2) \cdot M_{\operatorname{lv} \mathbb{C}}(K) = \\
&= (n-l-1) \cdot M_{\operatorname{lv} \mathbb{C}}(K)
\end{aligned}
\tag{28}
$$

(here we have used the fact that $m_{\operatorname{lv} f}(K) \leqslant M_{\operatorname{lv} \mathbb{C}}(K)$).

If $\operatorname{lv} \mathbb{C} < n$ and $|\operatorname{lv} \bar{\mathbb{C}}| = n$, we simply note that

$$
M(K) \leqslant M_{\operatorname{lv} \mathbb{C}}(K). \tag{29}
$$

Assume for simplicity that

$$
\operatorname{ld} \bar{\mathbb{C}} = \left\{ y_1^{(d_1)}, \ldots, y_k^{(d_k)} \right\},
$$

where $k = l$ or $k = l + 1$. Since all derivatives of y_i, $1 \leqslant i \leqslant k$, presented in $F \cup \mathbb{B} \cup H$ of order greater than d_i can be found among $\operatorname{rk} \mathbb{B}$, and since the elements of $\bar{F}$ and $\bar{H} \setminus H_{\mathbb{B}}$ are algebraic pseudo-remainders of G and H w.r.t. $\mathbb{B}$, we have

$$
m_i\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) \leqslant \begin{cases} d_i, & 1 \leqslant i \leqslant k \\ m_i(G \cup \mathbb{B} \cup H), & k < i \leqslant n. \end{cases} \tag{30}
$$

Also, recall that $\mathbb{B}$ satisfies the inequality (see (3))

$$
m_i(\mathbb{B}) \leqslant m_i\left(G \cup \bar{\mathbb{C}} \cup H\right) + \sum_{j=1}^{k} (m_j\left(G \cup \bar{\mathbb{C}} \cup H\right) - d_j), \ k < i \leqslant n. \tag{31}
$$

Combining (30) and (31), we obtain that

$$\begin{aligned}
M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right) &= (n-k)\sum_{i=1}^{k} d_i + \sum_{i=k+1}^{n} m_i\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right)\leqslant\\
&\leqslant (n-k)\sum_{i=1}^{k} d_i + \sum_{i=k+1}^{n} m_i(G\cup\mathbb{B}\cup H)\leqslant\\
&\leqslant (n-k)\sum_{i=1}^{k} d_i + \sum_{i=k+1}^{n} m_i\left(G\cup\bar{\mathbb{C}}\cup H\right)+\\
&\quad + (n-k)\sum_{j=1}^{k}(m_j\left(G\cup\bar{\mathbb{C}}\cup H\right)-d_j) =\\
&= (n-k)\sum_{i=1}^{k} m_i\left(G\cup\bar{\mathbb{C}}\cup H\right) + \sum_{i=k+1}^{n} m_i\left(G\cup\bar{\mathbb{C}}\cup H\right) =\\
&= M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(G\cup\bar{\mathbb{C}}\cup H\right)
\end{aligned}$$

and if $k=n$ then

$$M\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right)=\sum_{i=1}^{n} d_i + 0 = M\left(G\cup\bar{\mathbb{C}}\cup H\right)$$

because $\mathrm{rk}\,\bar{\mathbb{C}}=\mathrm{rk}\,\mathbb{B}^0$. Thus,

$$\begin{aligned}
&M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right)\leqslant M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(G\cup\bar{\mathbb{C}}\cup H\right),\ k<n\\
&M\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right)\leqslant M\left(G\cup\bar{\mathbb{C}}\cup H\right), \qquad k=n.
\end{aligned}\tag{32}$$

Now, applying (27), (28), or (29) with $K=G\cup\bar{\mathbb{C}}\cup H=F\cup\mathbb{C}\cup H$, we get

$$\begin{aligned}
M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right) &\leqslant M_{\mathrm{lv}\,\mathbb{C}}(F\cup\mathbb{C}\cup H), && l=k<n\\
M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right) &\leqslant (n-l-1)M_{\mathrm{lv}\,\mathbb{C}}\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right)\leqslant &&\\
&\leqslant (n-l-1)\cdot M_{\mathrm{lv}\,\mathbb{C}}(F\cup\mathbb{C}\cup H), && l<k<n\\
M\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right) &\leqslant M\left(G\cup\bar{\mathbb{C}}\cup H\right)= &&\\
&= M(F\cup\mathbb{C}\cup H)\leqslant &&\\
&\leqslant M_{\mathrm{lv}\,\mathbb{C}}(F\cup\mathbb{C}\cup H), && l<k=n\\
M\left(\bar{F}\cup\mathbb{B}^0\cup\bar{H}\right) &\leqslant M\left(G\cup\bar{\mathbb{C}}\cup H\right)= &&\\
&= M(F\cup\mathbb{C}\cup H), && l=k=n.
\end{aligned}\tag{33}$$

By taking into account the fact that invariant I5 holds for the triple $(F,\mathbb{C},H)$, we thus obtain this invariant for the triple $\left(\bar{F},\mathbb{B}^0,\bar{H}\right)$.

To conclude the proof of the bound for the output regular systems $\left(\mathbb{B}^0,\bar{H}\right)$, we note that it is already given by the invariant I5 when $k=n$, while in case $k<n$ we use inequality (29):

$$M\left(\mathbb{B}^0\cup\bar{H}\right)\leqslant M_{\mathrm{lv}\,\mathbb{B}^0}\left(\mathbb{B}^0\cup\bar{H}\right)\leqslant(n-1)!\cdot M(F_0\cup H_0).$$

□

4.3. Reduction-independent algorithm

In Algorithm 3 we had to be very careful in the reduction process. The idea was to emulate differential reductions by doing enough differentiations first and then applying purely algebraic reduction. We take care of the orders of derivatives in the first process and do not need to worry about them at the second algebraic step. Let us find out where the difficulties come from. If we use arbitrary d-triangular characteristic sets for reduction of polynomials, the result of reduction depends on the way of reduction very much.

Example 11 *Consider the following differential chain*

$$\mathbb{C} = x(x-1),\ (x-1)y,\ z+y+tx$$

with the elimination ranking $t < x < y < z$ and the differential polynomial

$$f = z' + y'.$$

We can reduce f w.r.t. $\mathbb{C}$ in many different ways and the remainders are very different:

(1)

$$z'+y' \xrightarrow{z'+y'+t'x+tx'} t'x+tx' \xrightarrow{(2x-1)x'} t'(2x-1)x = 2t'x^2 - t'x \longrightarrow$$
$$\xrightarrow{x^2-x} \quad t'x =: f_1$$

(2)

$$z'+y' \xrightarrow{(x-1)y'+x'y} (x-1)z' - x'y \xrightarrow{(x-1)y} (x-1)^2 z' \longrightarrow$$
$$\xrightarrow{z'+y'+t'x+tx'} (x-1)^2(y'+t'x+tx') \longrightarrow 0 =: f_2.$$

We see that the remainder f_1 depends on the variable t' that is not in both f_2 and $\mathbb{C}$. So, the reason for these so different answers is that the set $\mathbb{C}$ has a non-invertible initial. Speaking informally, if $\mathbb{C}$ is partially autoreduced and its initials and separants are invertible, then the result of reduction is more or less uniquely determined. In particular, the following result shows that all results of reduction of a polynomial w.r.t. a set with invertible initials and separants lie in a fixed Nötherian ring of algebraic polynomials.

Nevertheless, we do not have to restrict ourselves to partially autoreduced sets with invertible initials and separants. It turns out that, if we remove the latter restriction of invertibility, there still exists a fixed Nötherian subring $\mathbf{k}[X]$, with set X finite, satisfying the following property: if g is a remainder of f w.r.t. $\mathbb{C}$, then so is the truncation of g, which we define as the sum of those differential monomials in g that lie in $\mathbf{k}[X]$ (see Algorithm 4). So, whenever we find a remainder which does not belong to $\mathbf{k}[X]$, we can replace it by its truncation.

This is the key idea of Algorithm 5, which satisfies the same bound as Algorithm 3, yet does not require to replace differential pseudo-reduction by the algebraic one. In fact, procedure d-rem can compute any differential remainder in the following sense: within the scope of this section, let us call polynomial g a differential remainder of polynomial f w.r.t. $\mathbb{C}$, if g is reduced w.r.t. $\mathbb{C}$ and there exists $h \in H_{\mathbb{C}}^{\infty}$ such that

$$hf - g \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}.$$

Proposition 12 *Let $\mathbb{C}$ be partially autoreduced and coherent set of differential polynomials and f be a differential polynomial and g be a reduced w.r.t. $\mathbb{C}$ polynomial with*

$$hf - g \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$$

for some $h \in H_{\mathbb{C}}^{\infty}$. Let any differential polynomial $\bar{g}$, which is reduced w.r.t. $\mathbb{C}$, with

$$\bar{h}f - \bar{g} \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$$

for some $\bar{h} \in H_{\mathbb{C}}^{\infty}$ and $\bar{g} = a_k u^k + \ldots + a_0$ and u does not belong to the polynomial ring $\mathbf{k}[X]$ that contains both $\mathbb{C}$ and g. Then

$$\bar{g} - a_0 \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}.$$

Proof. Consider the differential polynomial

$$\bar{f} := \bar{h}(hf - g) - h(\bar{h}f - \bar{g}) = h\bar{g} - \bar{h}g \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}.$$

Since set $\mathbb{C}$ is partially autoreduced and coherent, ideal $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ is regular. The polynomial f is partially reduced w.r.t. $\mathbb{C}$. Therefore, by the Rosenfeld Lemma $\bar{f} \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$.

We have

$$\bar{f} = (h \cdot a_k)u^k + \ldots + (h \cdot a_0 - \bar{h} \cdot g)$$

with $\bar{h} \cdot g$ contributing only to a_0, because it does not depend on u. Since u does not appear in $\mathbb{C}$, the fact that $\bar{f} \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$ implies that every coefficient of $\bar{f}$ belongs to this ideal. In particular, $h \cdot a_k$ belongs to $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$, whence $a_i \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$, $1 \leqslant i \leqslant k$. Thus,

$$\bar{g} - a_0 = a_k u^k + \ldots + a_1 u \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}.$$

□

We are going to modify Algorithm 3, so that there is no necessity to replace differential pseudo-reduction by the algebraic one, as it was done in Algorithm 3 with the help of the Differentiate&Autoreduce procedure. However, the proof of the bound for the new Algorithm 5 is essentially based on that for Algorithm 3: in fact, based on the above Proposition 12, we will show that these algorithms satisfy the same bound.

Algorithm 4 Truncate $(f, \{p_i\})$

INPUT: *a differential polynomial f and numbers $p_i \geqslant 0$*

OUTPUT: **truncation** *of f, i.e., the sum of those terms of f that belong to the polynomial ring $R = \mathbf{k}[\ldots, y_i, \ldots, y_i^{(p_i)}, y_{i+1}, \ldots]$*

Let $f = \alpha_1 + \ldots + \alpha_q$, where α_i are differential monomials

$g := 0$

for $i := 1$ **to** q **do**

  if $\alpha_i \in R$ **then** $g := g + \alpha_i$

end for

return g

Algorithm 5 is obtained from Algorithm 3 via the following modification. In both algorithms we take a differentially triangular set $\mathbb{C}$, add to it the minimal element $f \in F$, which is reduced w.r.t. $\mathbb{C}$, and remove from $\mathbb{C}$ the polynomial with the same leading variable as f. As a result, we obtain a weak d-triangular set $\bar{\mathbb{C}}$. From now on, the two algorithms become different. Algorithm 3 computes a sufficient differential prolongation of $\bar{\mathbb{C}}$, and then computes algebraic pseudo-remainders w.r.t. it. Algorithm 5, instead, computes differential pseudo-remainders and then applies Proposition 12 to throw away the unnecessary parts of the remainders (which contain derivatives of high order).

Proposition 13 *Algorithm 5 is correct and satisfies the bound.*

Proof. The proof of correctness, termination, and bound for Algorithm 5 is based on the same invariants of the **while**-loop that were used for Algorithm 3. The only new step we make is the Truncate algorithm which is justified by Proposition 12. Indeed, we can obtain the remainder g appearing in Proposition 12 by applying Differentiate&Autoreduce and algrem; this remainder satisfies the bound. Hence, we can replace any other remainder by its truncation w.r.t. the bound. Let us explain this in detail.

We show that, for every differential remainder computed in the algorithm, its truncation is also a differential remainder in the sense of Proposition 12. Let

$$\mathbb{B} = \mathsf{Differentiate\&Autoreduce}\left(\bar{\mathbb{C}}, \left\{m_y\left(\bar{G}\right) \mid y \in \operatorname{lv}\bar{\mathbb{C}}\right\}\right).$$

We are going to show that the **for**-loop satisfies the following invariant. Take $C \in \bar{\mathbb{C}}$. Let

$$\mathbb{B}_{<C} = \{f \in \mathbb{B} \mid \operatorname{ld} f < \operatorname{ld} C\},$$

$B = \mathsf{algrem}(C, \mathbb{B}_{<C})$, $E = \mathsf{d\text{-}rem}(C, \mathbb{D})$, and $D = \mathsf{Truncate}\ (E, b)$. Then

$$\begin{aligned} h \cdot C - B &\in [\mathbb{D}] : H_{\mathbb{D}}^{\infty}, \\ B &\in [\mathbb{D} \cup \{D\}] : H_{\mathbb{D}}^{\infty}, \\ H_B &\subset (H_D^{\infty} + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}, \end{aligned}$$

for some $h \in H_{\mathbb{D}}^{\infty}$. We prove this statement by induction on the number of iterations of the **for**-loop.

Indeed, note that $B \in \mathbb{B}$. We have $h_1 \cdot C - B \in (\mathbb{B}_{<C})$ for some $h_1 \in H_{\mathbb{B}_{<C}}^{\infty}$. By induction we obtain that $[\mathbb{B}_{<C}] \subset [\mathbb{D}] : H_{\mathbb{D}}^{\infty}$. Hence,

$$h_1 \cdot C - B \in [\mathbb{D}] : H_{\mathbb{D}}^{\infty}.$$

Also by induction, $h_1 \in (H_{\mathbb{D}}^{\infty} + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}$. This means that there exist $h \in H_{\mathbb{D}}^{\infty}$, $h' \in H_{\mathbb{D}}^{\infty}$ such that $h \cdot h_1 - h' \in [\mathbb{D}]$. Thus,

$$h' \cdot C - B \in [\mathbb{D}] : H_{\mathbb{D}}^{\infty}.$$

From the properties of Algorithm Differentiate&Autoreduce, Lemma 4, and Proposition 12 we have the following inclusions:

$$B \in (\mathbb{B}_{<C} \cup \{C\}) \subset ([\mathbb{D}] : H_{\mathbb{D}}^{\infty} \cup \{E\}) \subset ([\mathbb{D}] : H_{\mathbb{D}}^{\infty} \cup \{D\}) \subset [\mathbb{D} \cup \{D\}] : H_{\mathbb{D}}^{\infty}$$

and

$$H_B \subset H_C + (\mathbb{B}_{<C}) \subset (H_E + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty} + [\mathbb{D}] : H_{\mathbb{D}}^{\infty} \subset (H_D + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}.$$

The same reasoning applies to the computation of sets $\bar{F}$ and $\bar{H}$. □

Algorithm 5 RGBound-Reduction-Independent(F_0, H_0)

INPUT: *finite sets of differential polynomials* $F_0 \neq \varnothing$ *and* H_0, *and a differential ranking*

OUTPUT: *a finite set* T *of regular systems such that*

$$\{F_0\} : H_0^\infty = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^\infty \quad \textit{and}$$

$$M(\mathbb{A} \cup H) \leqslant (n-1)!M(F_0 \cup H_0) \textit{ for } (\mathbb{A}, H) \in T.$$

$T := \varnothing, \quad U := \{(F_0, \varnothing, H_0)\}$

while $U \neq \varnothing$ **do**

Take and remove any $(F, \mathbb{C}, H) \in U$

f *an element of* F *of the least rank*

$D := \{C \in \mathbb{C} \mid \operatorname{lv} C = \operatorname{lv} f\}$

$G := F \cup D \setminus \{f\}$

$\bar{\mathbb{C}} := \mathbb{C} \setminus D \cup \{f\}$

$\bar{G} := G \cup \bar{\mathbb{C}} \cup H$

$$b := \left\{ m_y\left(\bar{G}\right) \mid y \in \operatorname{lv} \bar{C} \right\} \cup \left\{ m_z\left(\bar{G}\right) + \sum_{y \in \operatorname{lv} \bar{C}} \left(m_y\left(\bar{G}\right) - m_y\left(\operatorname{ld} \bar{\mathbb{C}}\right)\right) \mid z \notin \operatorname{lv} \bar{\mathbb{C}} \right\}$$

$\mathbb{D} := \varnothing$

for $C \in \bar{\mathbb{C}}$ *increasingly* **do**

$\mathbb{D} := \mathbb{D} \cup \{\mathsf{Truncate}\left(\mathsf{d\text{-}rem}\left(C, \mathbb{D}\right), b\right)\}$

if $\operatorname{rk} \mathbb{D} = \operatorname{rk} \bar{\mathbb{C}}$ **then**

$\bar{F} :=$ Truncate $(\mathsf{d\text{-}rem}(G, \mathbb{D}) \setminus \{0\}, b)$

$\bar{H} :=$ Truncate $(\mathsf{d\text{-}rem}(H \cup H_f, \mathbb{D}) \cup H_{\mathbb{D}}, b)$

if $\bar{F} \cap \mathbf{k} = \varnothing$ **and** $0 \notin \bar{H}$ **and** $\bar{F} = \varnothing$ **then**

$T := T \cup \{(\mathbb{D}, \bar{H})\}$ **else**

$U := U \cup \left\{\bar{F}, \mathbb{D}, \bar{H}\right\}$

$U := U \cup \{(F \cup H_f, \mathbb{C}, H)\}$

end while

return T

5. Transformation of characteristic sets of prime differential ideals

As above, let $\mathbf{k}\{Y\}$ be a ring of ordinary differential polynomials in n indeterminates with the differentiation δ. Let $\mathbb{C}$ be a characteristic set of a prime differential ideal I in $\mathbf{k}\{Y\}$ w.r.t. a ranking $\leq$. We propose an algorithm that computes a characteristic

set of I w.r.t. any other ranking $\leq'$ *algebraically*. More precisely, using a bound on the orders of derivatives occurring in the canonical characteristic set $\mathbb{D}$ of I w.r.t. the target ranking, we find a sufficient *differential prolongation* of $\mathbb{C}$ (described below), which defines a prime algebraic sub-ideal $\bar{I}$ in I containing $\mathbb{D}$. After that, it remains to compute an algebraic characteristic set of $\bar{I}$ w.r.t. the target ranking and extract from it a differential characteristic set of I.

5.1. A bound for characteristic sets of prime differential ideals

First, given a characteristic set $\mathbb{C}$ of a prime differential ideal I w.r.t. an arbitrary ranking $\leq$, we would like to obtain a bound on the orders of derivatives occurring in a characteristic set of I w.r.t. another given ranking $\leq'$. For $\leq$ orderly and $\leq'$ arbitrary, such a bound is given in Golubitsky et al. (2005). If $\leq$ is not orderly, we first obtain a bound for the orders of the elements of an orderly characteristic set $\mathbb{D}$ of I, and then apply the bound from Golubitsky et al. (2005).

Indeed, $\mathbb{D}$ can be computed from $\mathbb{C}$ with the help of the Rosenfeld-Gröbner algorithm applied to the system $F_0 = \mathbb{C}$, $H_0 = H_{\mathbb{C}}$ (where the initials and separants of $\mathbb{C}$ in $H_{\mathbb{C}}$ are taken w.r.t. $\leq$). Since I is prime, one of the regular components (A, H) computed by the Rosenfeld-Gröbner algorithm will coincide with I, and the characteristic set of the corresponding regular ideal $[A] : H^\infty$ w.r.t. $\leq'$ can be extracted from the lexicographic Gröbner basis of the algebraic ideal $(A) : H^\infty$ via the algorithm given in (Boulier et al., 1995, Theorem 6). A more efficient algorithm, which uses the fact that the given ideal is prime and thus avoids the computation of redundant regular components, is presented in Boulier et al. (2001).

Let M be the maximal order of derivatives occurring in $\mathbb{C}$. The only place where the Rosenfeld-Gröbner algorithm differentiates polynomials is the computation of differential pseudo-remainders. However, for an orderly ranking, the order of a polynomial cannot increase as a result of pseudo-reduction. Thus, the orders of derivatives occurring in the characteristic set $\mathbb{D}$ do not exceed M. In fact, the same applies to any other characteristic set of I w.r.t. the same orderly ranking: the leading derivatives of all characteristic sets of I w.r.t. the same ranking coincide, and the orders of non-leading derivatives occurring in a polynomial f cannot exceed the order of the leader of f w.r.t. an orderly ranking.

Now we will use the following

Lemma 14 *The number of elements in a characteristic set $\mathbb{C}$ of a prime differential ideal I in the ring of ordinary differential polynomials $\mathbf{k}\{y_1, \ldots, y_n\}$ does not depend on the ranking.*

Proof. If d is a differential dimension of P then the number of elements of $\mathbb{C}$ is equal to $n - d$ by (Cluzeau and Hubert, 2003, Theorem 4.11) which does not depend on a choice of a differential ranking. □

Remark 15 *The above lemma does not hold in the partial differential case. For example (borrowed from Boulier et al. (2001)), a characteristic set of the prime differential ideal*

$$[u_x^2 - 4u,\ u_{xy}v_y - u + 1,\ v_{xx} - u_x]$$

in $\mathbf{k}\{Y\}$ with derivations $\Delta = \{\partial/\partial x, \partial/\partial y\}$ may have 3 or 4 elements, depending on the ranking, but it takes a while to compute the characteristic set of the ideal w.r.t. the elimination ranking $u > v$ using the Rosenfeld-Gröbner algorithm in Maple (see Golubitsky (2006)).

Consider an example that requires less computation to achieve the result.

Example 16 *Consider the following prime differential ideal:*

$$P = [u_{yy},\ v_{xx} + y \cdot u_x + u].$$

This set of generators forms a characteristic set of P w.r.t. the elimination ranking with $v > u$. But, if we say that $u > v$ then the following set containing 3 elements will be a characteristic set of P :

$$\begin{aligned}
&v_{xxyyy},\\
&y^2 \cdot v_{xxxxyy} - 2y \cdot v_{xxxxy} + 2y \cdot v_{xxxyy} + 2v_{xxxx} - 2v_{xxxy} + v_{xxyy},\\
&2u - y^3 \cdot v_{xxxyy} + 2y^2 \cdot v_{xxxy} - 2y \cdot v_{xxx} + 2v_{xx}.
\end{aligned}$$

Applying Lemma 14, we obtain the following bound on the *order* of I (see Golubitsky et al. (2005)):

$$\operatorname{ord} I := \sum_{D \in \mathbb{D}} \operatorname{ord} D \leqslant |\mathbb{C}| \cdot \max_{C \in \mathbb{C}} \operatorname{ord} C. \tag{34}$$

This bound is likely to be non-optimal. It is possible that the results of (Ritt, 1950, Chapter VII), together with Lemma 14, imply the following bound, which is better: let $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_n$ be the numbers $m_y(\mathbb{C})$, $y \in Y$, arranged in non-increasing order, then

$$\operatorname{ord} I \leqslant \sum_{i=1}^{|\mathbb{C}|} m_i.$$

For this bound, which so far is a conjecture, one needs to verify that Ritt's proof holds for non-elimination rankings, and also adapt it for prime differential ideals specified by their characteristic sets, rather than sets of generators.

According to Golubitsky et al. (2005), the orders of derivatives occurring in the canonical characteristic set of I w.r.t. any ranking do not exceed the order of I. Thus, the number

$$M_1 = |\mathbb{C}| \cdot \max_{C \in \mathbb{C}} \operatorname{ord} C$$

bounds the orders of derivatives occurring in the canonical characteristic set of I w.r.t. any (not necessarily orderly) target ranking $\leq'$.

We note that the bound $(n-1)! \cdot M(\mathbb{C})$ obtained in Section 4.2 is also a bound for the orders of derivatives occurring in the characteristic set of I w.r.t. $\leq'$ computed by the Rosenfeld-Gröbner algorithm. In fact, invariant I5 in the proof of Proposition 10, together with Lemma 14, yields a better bound

$$M_2 = \frac{(n-1)!}{(n - |\mathbb{C}| - 1)!} \cdot M(\mathbb{C}).$$

In most cases, $M_2 > M_1$, but in some, especially for small values of n, it may happen that $M_2 < M_1$. This again suggests that none of the two bounds is optimal. Leaving the important problem of obtaining an optimal bound for future research, we summarize the bounds obtained so far in the following

Lemma 17 *Let $\mathbb{C}$ be a characteristic set of an ordinary prime differential ideal I w.r.t. a ranking $\leq$. Then* $\operatorname{ord} I$ *and the orders of derivatives occurring in the canonical characteristic set of I w.r.t. another ranking $\leq'$ do not exceed*

$$M_{\mathbb{C}} := \min(M_1, M_2) = \min\left(|\mathbb{C}| \cdot \max_{C \in \mathbb{C}} \operatorname{ord} C,\ \frac{(n-1)!}{(n - |\mathbb{C}| - 1)!} \cdot M(\mathbb{C})\right).$$

5.2. Differential prolongation: the prime case

Assume that $\mathrm{ld}_{\leq}\,\mathbb{C} = \left\{y_1^{(d_1)}, \ldots, y_k^{(d_k)}\right\}$. Let $m_i = M_{\mathbb{C}}$, $1 \leqslant i \leqslant k$. Compute the set

$$\mathbb{A} = \mathsf{Differentiate\&Autoreduce}\left(\mathbb{C}, \{m_i\}_{i=1}^{k}\right)$$

(for the algorithm Differentiate&Autoreduce, see Section 4.1 above).

Let $\mathbb{D}$ be the canonical characteristic set of I w.r.t. $\leq'$. Every polynomial in $\mathbb{D}$, as an element of I, reduces w.r.t. $\mathbb{C}$ and $\leq$ to zero. Since the orders of derivatives occurring in $\mathbb{D}$ do not exceed $M_{\mathbb{C}}$, every polynomial in $\mathbb{D}$ algebraically reduces to zero w.r.t. $\mathbb{A}$. That is, $\mathbb{D} \subset (\mathbb{A}) : H_{\mathbb{A}}^{\infty}$.

The algebraic ideal $\bar{I} = (\mathbb{A}) : H_{\mathbb{A}}^{\infty}$ is equal to the intersection of I with the ring $R = \mathbf{k}\left[\Theta Y \setminus \Theta\,\mathrm{ld}_{\leq}\,\mathbb{C} \cup \mathrm{ld}_{\leq}\,\mathbb{A}\right]$. Indeed, $\mathbb{A} \subset R$. Vice versa, every element of $I \cap R$ algebraically reduces w.r.t. $\mathbb{A}$ to zero and therefore belongs to $(\mathbb{A}) : H_{\mathbb{A}}^{\infty}$.

Since I is prime, so is $\bar{I}$. Applying one of the existing efficient algorithms (for instance, see Boulier et al. (2001) or Dahan et al. (2006)) to the set $\mathbb{A}$, we compute the canonical algebraic characteristic set $\mathbb{B}$ of $\bar{I}$ w.r.t. the target ranking $\leq'$. We know that the algebraic ideal $\bar{I}$ contains the canonical characteristic set $\mathbb{D}$ of the differential ideal I w.r.t. $\leq'$. In the following section, we will show that, in fact, $\mathbb{D} \subseteq \mathbb{B}$.

5.3. Extracting a differential characteristic set

The following two lemmas hold in the partial differential case. We assume that a ranking is fixed.

Lemma 18 *Let $\mathbf{k}\{Y\}$ be a ring of partial differential polynomials, and let K be an arbitrary subset of $\mathbf{k}\{Y\} \setminus \mathbf{k}$.*

Let $\mathbb{C}$ be a differential characteristic set of K and $\mathbb{A}$ an algebraic characteristic set of K. Let $\mathbb{T}$ be a weak d-triangular subset of $\mathbb{A}$ of the least rank. Then $\mathrm{rk}\,\mathbb{T} \leq \mathrm{rk}\,\mathbb{C}$.

Proof. Suppose that a polynomial $f \in \mathbb{C}$ is differentially reduced w.r.t. $\mathbb{T}$. Then, since $\mathbb{T}$ is a weak d-triangular subset of $\mathbb{A}$ of the least rank, f is algebraically reduced w.r.t. $\mathbb{A}$. Due to the fact that $\mathbb{A}$ is an algebraic characteristic set of K, we have $f = 0$, contradiction. Thus, no element of $\mathbb{C}$ is differentially reduced w.r.t. $\mathbb{T}$, which implies that $\mathrm{rk}\,\mathbb{T} \leq \mathrm{rk}\,\mathbb{C}$. □

Lemma 19 *Let I be a prime differential ideal, let $\mathbb{C}$ be the canonical characteristic set of I, and let $J = I \cap \mathbf{k}[V]$, where $V \subset \Theta Y$, be an algebraic ideal containing $\mathbb{C}$. Then the canonical algebraic characteristic set $\mathbb{D}$ of J contains $\mathbb{C}$; more precisely, $\mathbb{C}$ is the weak d-triangular subset of $\mathbb{D}$ of the least rank.*

Proof. Since $\mathbb{D}$ is triangular, its weak d-triangular subset of the least rank is unique. Let $\mathbb{T}$ be the weak d-triangular subset of $\mathbb{D}$ of the least rank.

Since $\mathbb{D}$ is an algebraic characteristic set of the prime ideal J, we have $H_{\mathbb{D}} \cap J = \varnothing$. Moreover, $H_{\mathbb{D}} \subset \mathbf{k}[V]$, therefore $H_{\mathbb{D}} \cap I = \varnothing$ and, hence, $H_{\mathbb{T}} \cap I = \varnothing$. Since $\mathbb{T} \subset I$ and I is prime, this implies

$$[\mathbb{T}] : H_{\mathbb{T}}^{\infty} \subset I. \tag{35}$$

Let

$$\mathbb{A} = \{\mathsf{d\text{-}rem}(f, \mathbb{T} \setminus \{f\}) \mid f \in \mathbb{T}\}.$$

Algorithm 6 Convert_Prime $(\mathbb{C}, \leq, \leq')$

INPUT: *a prime differential ideal* $P = [\mathbb{C}] : H_{\mathbb{C}}^{\infty} \subset \mathbf{k}\{y_1, \ldots, y_n\}$
with a characteristic set $\mathbb{C}$ *w.r.t. the input ranking* $\leq$
with leading variables $y_1, \ldots, y_k$ *and*
a target ranking $\leq'$.

OUTPUT: *canonical characteristic set of* P *w.r.t.* $\leq'$.

$M_{\mathbb{C}} := \min\left(|\mathbb{C}| \cdot \max\limits_{C \in \mathbb{C}} \operatorname{ord} C,\ \frac{(n-1)!}{(n-|\mathbb{C}|-1)!} \cdot M(\mathbb{C})\right)$

$m_i := M_{\mathbb{C}},\ 1 \leqslant i \leqslant k$

$\mathbb{A} :=$ Differentiate&Autoreduce $\left(\mathbb{C}, \{m_i\}_{i=1}^{k}\right)$

$\mathbb{D} :=$ Canonical_Algebraic_CharSet $((\mathbb{A}) : H_{\mathbb{A}}^{\infty}, \leq')$

return minimal d-triangular subset $(\mathbb{D}, \leq')$

We have $\mathbb{A} \subset [\mathbb{T}] \subset I$; we will show that set $\mathbb{A}$ is differentially autoreduced and $\operatorname{rk} \mathbb{A} = \operatorname{rk} \mathbb{T}$.

First, show that $\operatorname{rk} \mathbb{A} = \operatorname{rk} \mathbb{T}$. Indeed, suppose that for some $f \in \mathbb{T}$ and $g = \mathsf{d\text{-}rem}(f, \mathbb{T} \setminus \{f\})$, we have $\operatorname{rk} g < \operatorname{rk} f$. Since $\mathbb{T}$ is weak d-triangular, $\operatorname{ld} f \notin \Theta \operatorname{ld}(\mathbb{T} \setminus \{f\})$. Thus, Lemma 4 applies and tells us that $\mathbf{i}_f \in [\mathbb{T}] : H_{\mathbb{T}}^{\infty}$. Hence, according to (35), $\mathbf{i}_f \in I$. This contradicts with the fact that $H_{\mathbb{T}} \cap I = \varnothing$.

Now, since g is reduced w.r.t. $\mathbb{T} \setminus \{f\}$, $\operatorname{rk} g = \operatorname{rk} f$, and $\operatorname{rk} \mathbb{A} = \operatorname{rk} \mathbb{T}$, g is also reduced w.r.t. $\mathbb{A} \setminus \{g\}$. That is, set $\mathbb{A}$ is autoreduced.

By Lemma 18, $\operatorname{rk} \mathbb{T} \leq \operatorname{rk} \mathbb{C}$. Therefore, $\operatorname{rk} \mathbb{A} \leq \operatorname{rk} \mathbb{C}$. Since $\mathbb{A}$ is an autoreduced subset of I, while $\mathbb{C}$ is an autoreduced subset of I of the least rank, we have $\operatorname{rk} \mathbb{A} \geq \operatorname{rk} \mathbb{C}$. Thus, $\operatorname{rk} \mathbb{A} = \operatorname{rk} \mathbb{T} = \operatorname{rk} \mathbb{C}$.

Let $\bar{\mathbb{D}} = (\mathbb{D} \setminus \mathbb{T}) \cup \mathbb{C}$. Set $\bar{\mathbb{D}}$ is algebraically autoreduced, has the same rank as $\mathbb{D}$, and satisfies the requirements of canonicity: for every $f \in \bar{\mathbb{D}}$, the initial of f does not depend on the leaders of $\bar{\mathbb{D}}$, f is monic and has no factors in $\mathbf{k}[N(\bar{\mathbb{D}})]$, where $N(\bar{\mathbb{D}}) = N(\mathbb{D}) = V \setminus \operatorname{ld} \mathbb{D}$ is the set of non-leaders of $\mathbb{D}$ (or $\bar{\mathbb{D}}$). Since the canonical characteristic set is unique, we have $\bar{\mathbb{D}} = \mathbb{D}$ and $\mathbb{C} = \mathbb{T}$. This concludes the proof. □

Returning to the notation from the previous section and applying the above lemma, we obtain that the canonical characteristic set $\mathbb{D}$ of I is equal to the weak d-triangular subset of $\mathbb{B}$ of the least rank w.r.t. $\leq'$. This concludes the computation of the canonical characteristic set of I w.r.t. the target ranking, which we summarize in Algorithm 6.

6. Transformation of characteristic decompositions of radical differential ideals

We generalize the algebraic method for transforming characteristic sets of a prime differential ideal from one ranking to another to the case of a characterizable differential ideal. Since an ideal characterizable w.r.t. one ranking may not be characterizable w.r.t. another, we need to reformulate the problem: given a characterizable differential ideal I

with a characteristic set $\mathbb{C}$ w.r.t. a ranking $\leq$, compute a characteristic decomposition of I w.r.t. another ranking $\leq'$ *algebraically*. By analogy with the prime case, an algebraic computation here means finding a sufficient differential prolongation of $\mathbb{C}$, which defines a characterizable algebraic sub-ideal $\bar{I}$ in I, such that a differential characteristic decomposition of I w.r.t. $\leq'$ can be extracted from an algebraic characteristic decomposition of $\bar{I}$ w.r.t. $\leq'$.

We note that, given a characteristic decomposition of a radical differential ideal w.r.t. one ranking, we can obtain its characteristic decomposition w.r.t. another ranking algebraically by solving the above problem for each characterizable component.

All results of this section hold in the partial differential case, except for the bound in Section 6.2, which so far is known only for the ordinary case.

6.1. Differential prolongation

Definition 20 *Let F be a subset in a ring $\mathbf{k}\{Y\}$ of partial differential polynomials with a set of derivations Δ. A set $G \subset \Theta F$ is called a differential prolongation of F, if $F \subset G$ and the complement of G, $\Theta F \setminus G$, is invariant w.r.t. differentiation, i.e., for all $f \in \Theta F \setminus G$ and $\delta \in \Delta$, $\delta f \in \Theta F \setminus G$.*

A particular case of a differential prolongation of a weak d-triangular set F is F itself. If $F = \mathbb{C}$ is autoreduced and coherent then, according to (Kolchin, 1973, Lemma 6, page 137) and (Hubert, 2000, Lemma 6.1 and Theorem 6.2), the differential ideal $I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ is prime, respectively characterizable iff the algebraic ideal $J = (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$ is prime, respectively characterizable. The ideal J can be considered either as an algebraic ideal in the ring of differential polynomials $\mathbf{k}\{Y\}$ or as an ideal in the polynomial subring $\mathbf{k}[Z_{\mathbb{C}}]$, where $Z_{\mathbb{C}} = L \cup N$, $L = \operatorname{ld} \mathbb{C}$, $N = \Theta Y \setminus \Theta L$, since the fact that $\mathbb{C}$ is autoreduced implies $\mathbb{C} \subset \mathbf{k}[Z_{\mathbb{C}}]$. The Rosenfeld Lemma states that

$$[\mathbb{C}] : H_{\mathbb{C}}^{\infty} \cap \mathbf{k}[Z_{\mathbb{C}}] = (\mathbb{C}) : H_{\mathbb{C}}^{\infty},$$

where the latter ideal is considered in $\mathbf{k}[Z_{\mathbb{C}}]$. Moreover, a set $\mathbb{D}$ is a differential characteristic set of I iff $\mathbb{D}$ is an algebraic characteristic set of J (if the latter is considered in $\mathbf{k}[Z_{\mathbb{C}}]$, otherwise we need to impose an additional requirement that $\mathbb{D}$ is differentially autoreduced). In particular, the canonical characteristic sets of I and J (differential and algebraic, respectively) coincide (for this statement, it does not matter in which ring to consider J, since the canonical characteristic set of an ideal is the same regardless of the ring in which the ideal is considered).

Now, if we consider a differential prolongation $\mathbb{D}$ of $\mathbb{C}$ and the corresponding polynomial subring $\mathbf{k}[Z_{\mathbb{D}}]$, where $Z_{\mathbb{D}} = \bar{L} \cup N$, $\bar{L} = \operatorname{ld} \mathbb{D}$, $N = \Theta Y \setminus \Theta L = \Theta Y \setminus \Theta \bar{L}$, then $\mathbb{D}$ is not necessarily a subset of $\mathbf{k}[Z_{\mathbb{D}}]$:

Example 21 *Let $\mathbb{C} = y'$, $x + y$ with the elimination ranking $y < x$ and a prolongation*

$$\mathbb{D} = y',\ x + y,\ x' + y',\ x'' + y''.$$

Then

$$\bar{L} = y',\ x,\ x',\ x'', \quad N = y.$$

Hence, we have that $x'' + y'' \notin \mathbf{k}[Z_{\mathbb{D}}]$. Also,

$$[\mathbb{C}] : H_{\mathbb{C}}^{\infty} \cap \mathbf{k}[Z_{\mathbb{D}}] = (y',\ x + y,\ x',\ x'')$$

and $x'' \notin (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$.

Therefore, we need to distinguish between two ideals $I_{\mathbb{D}} := (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$ in $\mathbf{k}\{Y\}$ and $\bar{I}_{\mathbb{D}} := I \cap \mathbf{k}[Z_{\mathbb{D}}]$ in $\mathbf{k}[Z_{\mathbb{D}}]$.

The algebraic ideal $\bar{I}_{\mathbb{D}}$ depends only on the set of leaders $\bar{L}$ of the differential prolongation of $\mathbb{C}$. In other words, for any characterizing set $\tilde{\mathbb{C}}$ of I and its differential prolongation $\tilde{\mathbb{D}}$ with $\operatorname{ld}\tilde{\mathbb{D}} = \operatorname{ld}\mathbb{D} = \bar{L}$, we have $\bar{I}_{\tilde{\mathbb{D}}} = \bar{I}_{\mathbb{D}}$. We call $\bar{I}_{\bar{L}} := \bar{I}_{\mathbb{D}}$ a *prolongation ideal* of the ideal I.

Next, we study the properties of the prolongation ideals. The following lemma gives a criterion for a prolongation ideal to be prime or characterizable.

Lemma 22 *Let $\mathbb{C}$ be a coherent autoreduced set, and let $\mathbb{D}$ be a differential prolongation of $\mathbb{C}$. Then the differential ideal $1 \notin I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ is prime, respectively characterizable, iff the corresponding prolongation ideal $\bar{I}_{\mathbb{D}}$ is prime, respectively characterizable.*

Proof. If I is prime then its restriction $I \cap \mathbf{k}[Z_{\mathbb{D}}] = \bar{I}_{\mathbb{D}}$ is also prime. If $\bar{I}_{\mathbb{D}}$ is prime than its restriction $\bar{I}_{\mathbb{D}} \cap \mathbf{k}[Z_{\mathbb{C}}] = (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$ is prime and, thus, I is prime.

Let I be a characterizable differential ideal. We will show that set $\mathbb{A}$ given by formula (36) characterizes the prolongation ideal $\bar{I}_{\mathbb{D}}$. We have $\bar{I}_{\mathbb{D}} \subset (\mathbb{A}) : H_{\mathbb{A}}^{\infty}$. Indeed, by Lemma 4, sets $\mathbb{A}$ and $\mathbb{D}$ have the same ranks, whence they have the same sets of reduced polynomials. In particular, since $\mathbb{D}$ is a differential prolongation of the characteristic set $\mathbb{C}$, the ideal $\bar{I}_{\mathbb{D}}$ has no non-zero polynomials reduced w.r.t. $\mathbb{D}$, and hence w.r.t. $\mathbb{A}$.

Now note that $(\mathbb{A}) : H_{\mathbb{A}}^{\infty} \subset I$ and $\mathbb{A} \subset \mathbf{k}[Z_{\mathbb{D}}]$. Hence, $\bar{I}_{\mathbb{D}} = (\mathbb{A}) : H_{\mathbb{A}}^{\infty}$ and $\mathbb{A}$ is a characteristic set of $\bar{I}_{\mathbb{D}}$. Thus, $\bar{I}_{\mathbb{D}}$ is characterizable.

Since $\mathbb{C} \subset \mathbf{k}[Z_{\mathbb{D}}]$ and $(\mathbb{C}) : H_{\mathbb{C}}^{\infty} = I \cap \mathbf{k}[Z_{\mathbb{C}}]$, we have

$$(\mathbb{C}) : H_{\mathbb{C}}^{\infty} = (\mathbb{A}) : H_{\mathbb{A}}^{\infty} \cap \mathbf{k}[Z_{\mathbb{C}}].$$

□

The next lemma establishes a relation between the characteristic sets of a characterizable differential ideal I and the algebraic characteristic sets of its prolongation ideals.

Lemma 23 *Let $\mathbb{C}$ be a characteristic set of the differential ideal $1 \notin I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$, let $\bar{L}$ be a differential prolongation of $L = \operatorname{ld}\mathbb{C}$, and let $\bar{I}_{\bar{L}}$ be the corresponding prolongation ideal.*

Then a characterizing set $\mathbb{A}$ of $\bar{I}_{\bar{L}}$ can be obtained from $\mathbb{C}$ as

$$\mathbb{A} := \{\mathsf{algrem}(f, \mathbb{B} \setminus \{f\}) \mid f \in \mathbb{B},\ \operatorname{ld} f \in \bar{L}\}, \tag{36}$$

where $\mathbb{B}$ is any triangular subset of $\Theta\mathbb{C}$ satisfying $\operatorname{ld}\mathbb{B} = \operatorname{ld}\Theta\mathbb{C}$.

Vice versa, given a characterizing set $\mathbb{A}$ of $\bar{I}_{\bar{L}}$, let $\mathbb{T}$ be a weak d-triangular subset of $\mathbb{A}$ of the least rank. If $\mathbb{T}$ is differentially autoreduced, then it is a characterizing set of I. In particular, if $\mathbb{A}$ is the canonical characteristic set of $\bar{I}_{\bar{L}}$, then $\mathbb{T}$ is the canonical characteristic set of I.

Proof. Since I is characterizable, $\bar{I}_{\bar{L}}$ is also characterizable by Lemma 22 and $\mathbb{A}$ is its characteristic set. The other way follows from Lemma 18. □

In the ordinary case, the triangular set $\mathbb{B}$ considered in the above lemma is unique. Moreover, set $\mathbb{A}$ can be equivalently obtained as

$$\mathbb{A} := \mathsf{Differentiate\&Autoreduce}(\mathbb{C}, \{m_i\}),$$

where the numbers $\{m_i\}$ are the maximal orders of derivatives of the leading differential indeterminates of $\mathbb{C}$ occurring in the prolongation $\bar{L}$. It is preferable to compute $\mathbb{A}$ in this way, because Differentiate&Autoreduce provides a bound on the orders of non-leading derivatives occurring in $\mathbb{A}$, which can be used for establishing complexity estimates for the entire transformation algorithm.

A generalization of Algorithm Differentiate&Autoreduce to the partial case is an interesting open problem. Moreover, in the partial case, there may be uncountably infinitely many triangular subsets of $\Theta\mathbb{C}$ whose leaders coincide with $\operatorname{ld}\Theta\mathbb{C}$. Thus, not every such set can be enumerated by an algorithmic procedure. However, it is easy to write a procedure that would enumerate a particular subset of $\Theta\mathbb{C}$, given $\mathbb{C}$; this procedure makes the computation of the set of algebraic pseudo-remainders algorithmic as well. If one would like to choose the subset $\mathbb{B}$ in a systematic way, we suggest to use the ideas from the theory of monomial involutive divisions (see Gerdt and Blinkov (1998)).

According to (Hubert, 2003, Theorem 4.13), there is a one-to-one correspondence between the essential prime components of a characterizable differential ideal $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ and the minimal prime components of the corresponding algebraic ideal $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$. The following lemma generalizes this result to prolongation ideals.

Lemma 24 *Let $\mathbb{C}$ be a characteristic set of the differential ideal $I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$, let $\bar{L}$ be a differential prolongation of $L = \operatorname{ld}\mathbb{C}$, and let $\bar{I}_{\bar{L}}$ be the corresponding prolongation ideal.*

Let $I = P_1 \cap \ldots \cap P_k$ be the essential prime decomposition of I, then

$$\bar{I}_{\bar{L}} = (\bar{P}_1)_{\bar{L}} \cap \ldots \cap (\bar{P}_k)_{\bar{L}}$$

is the minimal prime decomposition of the prolongation ideal.

Proof. Since $\bar{I}_{\bar{L}} = I \cap \mathbf{k}[Z_{\bar{L}}]$,

$$\bar{I}_{\bar{L}} = (P_1 \cap \mathbf{k}[Z_{\bar{L}}]) \cap \ldots \cap (P_k \cap \mathbf{k}[Z_{\bar{L}}]) = (\bar{P}_1)_{\bar{L}} \cap \ldots \cap (\bar{P}_k)_{\bar{L}}$$

is a prime decomposition of the ideal $\bar{I}_{\bar{L}}$. Suppose that it is not minimal. Since $(\mathbb{C}) : H_{\mathbb{C}}^{\infty} = \bar{I}_{\bar{L}} \cap \mathbf{k}[Z_{\mathbb{C}}]$,

$$(\mathbb{C}) : H_{\mathbb{C}}^{\infty} = \big((\bar{P}_1)_{\bar{L}} \cap \mathbf{k}[Z_{\mathbb{C}}]\big) \cap \ldots \cap \big((\bar{P}_k)_{\bar{L}} \cap \mathbf{k}[Z_{\mathbb{C}}]\big)$$

is a prime decomposition of the ideal $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$, which is also not minimal. But the latter contradicts the fact that $(\bar{P}_i)_{\bar{L}} \cap \mathbf{k}[Z_{\mathbb{C}}] = P_i \cap \mathbf{k}[Z_{\mathbb{C}}]$, $1 \leqslant i \leqslant k$, and

$$(\mathbb{C}) : H_{\mathbb{C}}^{\infty} = (P_1 \cap \mathbf{k}[Z_{\mathbb{C}}]) \cap \ldots \cap (P_k \cap \mathbf{k}[Z_{\mathbb{C}}])$$

is the minimal prime decomposition. □

6.2. A bound for characteristic sets of prime components

Let $I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ be a characterizable differential ideal with a characteristic set $\mathbb{C}$ w.r.t. a ranking $\leq$. Let $L = \operatorname{ld}_{\leq}\mathbb{C}$, and let $\bar{L}$ be a differential prolongation of L. From the previous section we know that the prolongation ideal $\bar{I}_{\bar{L}}$ is characterizable (Lemma 22) and its minimal prime components correspond to the essential prime components of I (Lemma 24). We would like to find a sufficient differential prolongation $\bar{L}$ such that the minimal prime components of $\bar{I}_{\bar{L}}$ contain differential characteristic sets of the corresponding essential prime components of I w.r.t. any other ranking $\leq'$.

First of all, according to (Hubert, 2003, Theorem 4.13), a differential characteristic set of an essential prime component of I coincides with an algebraic characteristic set of the corresponding minimal prime component of the ideal $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$. This implies that every essential prime component P of I has a characteristic set $\mathbb{C}_P$ satisfying the bound $m_y(\mathbb{C}_P) \leqslant m_y(\mathbb{C})$ on the orders of derivatives of any differential indeterminate $y \in Y$ occurring in $\mathbb{C}_P$.

For the ordinary case, as was shown in Section 5.1, we thus have a bound $M_{\mathbb{C}}$ on the orders of derivatives occurring in the canonical characteristic sets of the essential prime components of I w.r.t. any other ranking $\leq'$. For the partial differential case, such a bound is not known, but let us assume that we can compute such a bound $M_{\mathbb{C}}$ also for the partial case.[6] We need to assume that $M_{\mathbb{C}} \geqslant m_y(\mathbb{C})$ for all $y \in Y$.

Let

$$\bar{L} = \{\theta u \mid u \in L,\ \operatorname{ord} \theta u \leqslant M_{\mathbb{C}}\} \tag{37}$$

be the differential prolongation of L up to the order $M_{\mathbb{C}}$. According to Lemma 24, the minimal prime components of $\bar{I}_{\bar{L}}$ contain all polynomials of the corresponding essential prime components of I of order less than or equal to $M_{\mathbb{C}}$. Thus, they also contain the canonical characteristic sets of the corresponding essential prime components of I w.r.t. any other ranking $\leq'$. In what follows, we will denote the above differential prolongation $\bar{I}_{\bar{L}}$ simply by $\bar{I}$. Applying Lemma 23, we compute a characteristic set of $\bar{I}$ w.r.t. $\leq$.

6.3. Algebraic bi-characteristic decomposition

So, we have the differential ideal I which is characterizable w.r.t. the ranking $\leq$ and would like to give a characteristic decomposition of I w.r.t. $\leq'$. We have constructed the prolongation algebraic ideal $\bar{I}$ which is characterizable w.r.t. $\leq$ with a characteristic set $\mathbb{A}$ given by formula (36). Let

$$\bar{I} = \bar{J}_1 \cap \ldots \cap \bar{J}_k \tag{38}$$

be a bi-characteristic decomposition of $\bar{I}$ w.r.t. $\leq$ and $\leq'$. That is, each component $\bar{J}_i$, $1 \leqslant i \leqslant k$, is an algebraic ideal characterizable w.r.t. both rankings with the canonical characteristic sets $\mathbb{A}_i$ and $\mathbb{B}_i$ w.r.t. $\leq$ and $\leq'$, respectively.

Let us discuss how one can construct such a decomposition. Algorithm 7 does the following. Given a characterizable algebraic ideal I w.r.t. $\leq$, it first computes its algebraic characteristic decomposition w.r.t. $\leq'$. This can be done by by applying the *Triade* algorithm by Moreno Maza (1999), which is implemented in the `RegularChains` library in Maple (see Lemaire et al. (2005)). A parallel implementation of this algorithm, on a shared memory machine in `Aldor` is also in progress (see Moreno Maza and Xie (2006)).

If one of the characterizable components turns out to be equal to I (note that equality of characterizable algebraic ideals can be checked, e.g., by computing their Gröbner bases), then I is bi-characterizable; in this case the algorithm terminates and outputs T consisting of a single pair $(\mathbb{C}, \mathbb{D})$ of characterizing sets of I w.r.t. $\leq$ and $\leq'$, respectively. If all characterizable components of I contain it strictly, then, for each characterizable component, we compute its characteristic decomposition w.r.t. $\leq$ and repeat the above strategy.

[6] Of course, $M_{\mathbb{C}}$ can be obtained by computing characteristic sets of the prime components w.r.t. the target ranking, but this would clearly defeat our purpose: we need a bound that can be computed from $\mathbb{C}$ relatively easily.

Algorithm 7 Algebraic-Bicharacteristic-Decomposition $(\mathbb{C}, \leq, \leq')$

INPUT: *characterizing set* $\mathbb{C}$ *of a characterizable algebraic ideal* I
w.r.t. an ordering $\leq$ *on variables*
and another ordering $\leq'$

OUTPUT: *a finite set* $T = \{(\mathbb{C}_i, \mathbb{D}_i) \mid i \in \mathfrak{I}\}$, *where*
for every $i \in \mathfrak{I}$, $\mathbb{C}_i$ *and* $\mathbb{D}_i$ *are algebraic characterizing sets*
of the same ideal I_i *w.r.t.* $\leq$ *and* $\leq'$, *respectively, and*
$I = \cap_{i \in \mathfrak{I}} I_i$

$\leq_s := \leq$, $\leq_t := \leq'$
$\mathfrak{C} := \{\mathbb{C}\}$, $T := \varnothing$
while $\mathfrak{C} \neq \varnothing$ **do**
$U := \mathfrak{C}$, $\mathfrak{C} := \varnothing$
for $\mathbb{C} \in U$ **do**
$J := (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$ *w.r.t.* $\leq_s$
$\mathfrak{D} :=$*Algebraic-characteristic-decomposition*$(\mathbb{C}, \leq_s, \leq_t)$
if $\exists\, \mathbb{D} \in \mathfrak{D}$ *such that* $J = (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$ *w.r.t.* $\leq_t$ **then**
if $\leq_s = \leq$ **then** $T := T \cup \{(\mathbb{C}, \mathbb{D})\}$ **else** $T := T \cup \{(\mathbb{D}, \mathbb{C})\}$
else $\mathfrak{C} := \mathfrak{C} \cup \mathfrak{D}$
end if
end for
if $\leq_s = \leq$ **then** $\leq_s := \leq'$, $\leq_t := \leq$ **else** $\leq_s := \leq$, $\leq_t := \leq'$
end while
return T

Correctness of the algorithm follows from the fact that, at each iteration of the **while**-loop, $\mathfrak{C} \cup T$ provides a characteristic decomposition of I w.r.t. $\leq_s$ and T satisfies the requirements of the output. Termination follows from the Nötherian property of the polynomial ring, i.e., that every sequence of strictly nested polynomial ideals is finite.

We note that components $\bar{J}_i$, for which $\mathrm{ld}_{\leq} \mathbb{A}_i \neq \mathrm{ld}_{\leq} \mathbb{A}$, are redundant, i.e., they can be excluded from the right-hand side of (38) without affecting the intersection. Indeed, if $\bar{I} = \bar{P}_1 \cap \ldots \cap \bar{P}_l$ is the minimal prime decomposition of $\bar{I}$, and $\bar{J}_i = \bar{Q}_{i,1} \cap \ldots \cap \bar{Q}_{i,l_i}$ are the minimal prime decompositions of $\bar{J}_i$, $1 \leqslant i \leqslant k$, then a component $\bar{J}_i$ is redundant, if none of $\bar{P}_j$, $1 \leqslant j \leqslant l$, can be found among $\bar{Q}_{i,t}$, $1 \leqslant t \leqslant l_i$. But this is the case if $\mathrm{ld}_{\leq} \mathbb{A}_i \neq \mathrm{ld}_{\leq} \mathbb{A}$, since by (Hubert, 2003, Theorem 4.13) the characteristic sets of $\bar{P}_j$ have leaders $\mathrm{ld}_{\leq} \mathbb{A}$, while the characteristic sets of $\bar{Q}_{i,t}$ have leaders $\mathrm{ld}_{\leq} \mathbb{A}_i$. Therefore, we can

assume that for all $1 \leqslant i \leqslant k$, $\mathrm{ld}_{\leq} \mathbb{A}_i = \mathrm{ld}_{\leq} \mathbb{A}$.

We prove then that *every* minimal prime component of $\bar{J}_i$ is a minimal prime component of $\bar{I}$. Indeed, every $\bar{Q}_{i,t}$ is a prime ideal containing $\bar{I}$. Suppose that $\bar{Q}_{i,t}$ is not minimal, i.e., there is a minimal prime component $\bar{P}_j$ of $\bar{I}$ such that $\bar{P}_j \subsetneq \bar{Q}_{i,t}$. But the latter strict inclusion is impossible according to the following Lemma 25 and Remark 26.

Lemma 25 *Let P and Q be two prime differential ideals whose characteristic sets w.r.t. $\leq$ have the same sets of leaders. Then $P \subseteq Q$ implies $P = Q$.*

Proof. Let $\mathbb{C}_1$ and $\mathbb{C}_2$ be these characteristic sets. We have $P = [\mathbb{C}_1] : H^{\infty}_{\mathbb{C}_1}$ and $Q = [\mathbb{C}_2] : H^{\infty}_{\mathbb{C}_2}$. Consider the restricted ideals $\mathfrak{p} = (\mathbb{C}_1) : H^{\infty}_{\mathbb{C}_1}$ and $\mathfrak{q} = (\mathbb{C}_2) : H^{\infty}_{\mathbb{C}_2}$ in the Nötherian ring $\mathbf{k}[L, N(\mathbb{C}_1, \mathbb{C}_2)]$ where $N(\mathbb{C}_1, \mathbb{C}_2)$ is the set of non-leading variables appearing in both $\mathbb{C}_1$ and $\mathbb{C}_2$. From (Hubert, 2000, Theorem 3.2) it follows that both $\mathfrak{p}$ and $\mathfrak{q}$ are of dimension $|N(\mathbb{C}_1, \mathbb{C}_2)|$.

Take any $f \in \mathfrak{p}$. It is partially reduced w.r.t. both $\mathbb{C}_1$ and $\mathbb{C}_2$ (which are coherent and autoreduced) and belongs to $P \subset Q$. By the Rosenfeld lemma $f \in \mathfrak{q}$. Hence, $\mathfrak{p} \subset \mathfrak{q}$ and they are prime and must be equal then, because their Krull dimensions are equal to the same number $|N(\mathbb{C}_1, \mathbb{C}_2)|$. Hence, we have $\mathbb{C}_1 \subset Q$ and $\mathbb{C}_2 \subset \mathfrak{p} \subset P$ at the same time. Thus, according to (Golubitsky et al., 2005, Theorem 9) we finally obtain that $P = Q$. $\square$

Remark 26 *In the above lemma, one can assume that the set of derivations is empty, hence the statement also holds for algebraic ideals.*

To summarize, for every bi-characterizable component $\bar{J}_i$, there exists a subset $T_i \subset \{1, \ldots, l\}$ such that

$$\bar{J}_i = \bigcap_{j \in T_i} \bar{P}_j$$

is the minimal prime decomposition of $\bar{J}_i$. Moreover, equality (38) implies that

$$\bigcup_{i=1}^{l} T_i = \{1, \ldots, l\}.$$

6.4. Constructing differential characterizable components from the algebraic ones

Fix any of the above algebraic bi-characterizable components $\bar{J} = \bar{J}_i$, where $1 \leqslant i \leqslant k$; we have a set of indices $T = T_i \subset \{1, \ldots, l\}$ such that

$$\bar{J} = \bigcap_{j \in T} \bar{P}_j.$$

As above, let $\mathbb{A} = \mathbb{A}_i$ and $\mathbb{B} = \mathbb{B}_i$ be the canonical characteristic sets of $\bar{J}$ w.r.t. $\leq$ and $\leq'$, respectively.

According to Lemma 24, each minimal prime component $\bar{P}_j$ of $\bar{I}$ is a prolongation ideal of the corresponding essential prime component P_j of I, i.e.,

$$\bar{P}_j = P_j \cap \mathbf{k}[\bar{L} \cup N],$$

where $I = \bigcap_{j=1}^{l} P_j$ is the essential prime decomposition of I. Since $\mathbb{B}$ is a characterizing set of $\bar{J}$ w.r.t. $\leq'$, the initials and separants of $\mathbb{B}$ w.r.t. $\leq'$ are not zero-divisors modulo

$\bar{J}$, i.e., they do not belong to the minimal prime components $\bar{P}_j$, $j \in T$. Since $\mathbb{B}$, as well as $H_{\mathbb{B}}$, is a subset of $\mathbf{k}[\bar{L} \cup N]$, we have therefore $H_{\mathbb{B}} \cap P_j = \varnothing$, $j \in T$.

Let $\mathbb{T} \subset \mathbb{B}$ be the weak d-triangular subset of $\mathbb{B}$ of the least rank w.r.t. $\leq'$. Since $H_{\mathbb{T}} \subset H_{\mathbb{B}}$, we also have $H_{\mathbb{T}} \cap P_j = \varnothing$, $j \in T$. Thus, $[\mathbb{T}] : H_{\mathbb{T}}^{\infty} \subset P_j$, $j \in T$. In particular, this implies that $[\mathbb{T}] : H_{\mathbb{T}}^{\infty} \neq (1)$.

Let $\mathbb{D}$ be the result of differential autoreduction of $\mathbb{T}$ w.r.t. $\leq'$, i.e.,

$$\mathbb{D} = \{\mathsf{d\text{-}rem}(f, \mathbb{T} \setminus \{f\}) \mid f \in \mathbb{T}\}.$$

Set $\mathbb{D}$ is differentially autoreduced. By definition of differential remainder, $\mathbb{D} \subset [\mathbb{T}]$. By Lemma 4, since $[\mathbb{T}] : H_{\mathbb{T}}^{\infty} \neq (1)$, we have $\mathrm{rk}_{\leq'} \mathbb{D} = \mathrm{rk}_{\leq'} \mathbb{T}$ and, moreover, $H_{\mathbb{D}} \subset H_{\mathbb{T}}^{\infty} + [\mathbb{T}]$. Therefore,

$$[\mathbb{D}] : H_{\mathbb{D}}^{\infty} \subset [\mathbb{T}] : H_{\mathbb{T}}^{\infty} \subset P_j, \;\; j \in T. \tag{39}$$

We will show that $\mathbb{D}$ is a characteristic set of the ideal $[\mathbb{D}] : H_{\mathbb{D}}^{\infty}$ w.r.t. $\leq'$ by proving that every polynomial in the intersection $\bigcap_{j \in T_i} P_j$ reduces w.r.t. $\mathbb{D}$ to zero. Given (39), this will also imply that

$$[\mathbb{D}] : H_{\mathbb{D}}^{\infty} = \bigcap_{j \in T} P_j. \tag{40}$$

Take any polynomial $f \in \bigcap_{j \in T} P_j$, and let $\bar{f} = \mathsf{d\text{-}rem}(f, \mathbb{D})$, where the pseudo-remainder is computed w.r.t. $\leq'$. Since $\mathbb{D} \subset [\mathbb{T}] \subset P_j$, $j \in T$, we have $\bar{f} \in \bigcap_{j \in T} P_j$.

Let $\mathbb{F}_j$ be the canonical characteristic set of P_j w.r.t. $\leq'$, and let $\bar{\mathbb{F}}_j$ be the canonical algebraic characteristic set of the corresponding prolongation ideal $\bar{P}_j$. We have shown in Section 6.2 that $\bar{P}_j$ contains $\mathbb{F}_j$. Thus, from Lemma 19 it follows that $\mathbb{F}_j$ is the weak d-triangular subset of $\bar{\mathbb{F}}_j$ of the least rank w.r.t. $\leq'$. On the other hand, since $\bar{P}_j$ is a minimal prime component of $\bar{J}$, according to (Hubert, 2003, Theorem 4.13), $\mathrm{ld}_{\leq'} \bar{\mathbb{F}}_j = \mathrm{ld}_{\leq'} \mathbb{B}$. This implies that $\mathrm{ld}_{\leq'} \mathbb{F}_j = \mathrm{ld}_{\leq'} \mathbb{T} = \mathrm{ld}_{\leq'} \mathbb{D}$. That is, the fact that $\bar{f}$ is reduced w.r.t. $\mathbb{D}$ implies that it is partially reduced w.r.t. $\mathbb{F}_j$.

By the Rosenfeld Lemma,

$$\bar{f} \in (\mathbb{F}_j) : H_{\mathbb{F}_j}^{\infty} \subset (\bar{\mathbb{F}}_j) : H_{\bar{\mathbb{F}}_j}^{\infty} = \bar{P}_j, \;\; j \in T$$

i.e., $\bar{f} \in \bar{J}$. Now, the fact that $\bar{f}$ is reduced w.r.t. $\mathbb{D}$ implies that it is algebraically reduced w.r.t. $\mathbb{B}$. Since the latter is a characteristic set of $\bar{J}$, we obtain $\bar{f} = 0$ and the required equality (40).

Now we see that the ideal $[\mathbb{D}] : H_{\mathbb{D}}^{\infty}$ is characterizable w.r.t. $\leq'$. The canonical characteristic set of this ideal w.r.t. $\leq'$ is contained in each minimal prime component of the ideal $(\mathbb{D}) : H_{\mathbb{D}}^{\infty}$, therefore it is also contained in every $\bar{P}_j$, $j \in T$, and hence in $\bar{J}$. The ideal $\bar{J}$ is contained in $[\mathbb{D}] : H_{\mathbb{D}}^{\infty}$. Thus, by Lemma 19, the canonical characteristic set of $[\mathbb{D}] : H_{\mathbb{D}}^{\infty}$ is equal to the weak d-triangular subset of $\mathbb{B}$ of the least rank w.r.t. $\leq'$. That is, we have

$$\mathbb{D} = \mathbb{T}$$

which is (w.r.t. the ranking $\leq'$) the canonical characteristic set of the characterizable differential ideal

$$[\mathbb{D}] : H_{\mathbb{D}}^{\infty}.$$

Algorithm 8 Convert_Characterizable $(\mathbb{C}, \leq, \leq')$

INPUT: *set* $\mathbb{C}$ *which characterizes the ideal* $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ *w.r.t. the input ranking* $\leq$ *and has leading variables* $y_1, \ldots, y_k$ *and a target ranking* $\leq'$.

OUTPUT: *characteristic decomposition of* $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ *w.r.t.* $\leq'$.

$M_{\mathbb{C}} := \min\left(|\mathbb{C}| \cdot \max_{C \in \mathbb{C}} \operatorname{ord} C,\ \frac{(n-1)!}{(n-|\mathbb{C}|-1)!} \cdot M(\mathbb{C})\right)$

$m_i := M_{\mathbb{C}},\ 1 \leqslant i \leqslant k$

$\mathbb{A} :=$ Differentiate&Autoreduce $\left(\mathbb{C}, \{m_i\}_{i=1}^{k}\right)$

$\mathfrak{D} :=$ Bi-characterizable_Canonical_Decomposition $((\mathbb{A}) : H_{\mathbb{A}}^{\infty}, \leq, \leq')$

$\mathfrak{C} := \{\text{minimal d} - \text{triangular subset } (\mathbb{D}, \leq') \mid \mathbb{D} \in \mathfrak{D}\}$

return $\mathfrak{C}$

6.5. The final characteristic decomposition

In the previous section, we have shown that for each bi-characterizable component $\bar{J}_i$, $1 \leq i \leq l$, of $\bar{I}$ with the canonical characteristic set $\mathbb{B}_i$ w.r.t. $\leq'$, if $\mathbb{D}_i$ is the weak d-triangular subset of $\mathbb{B}_i$ of the least rank, then it is the canonical characteristic set of the ideal $[\mathbb{D}_i] : H_{\mathbb{D}_i}^{\infty}$. We have also shown that

$$[\mathbb{D}_i] : H_{\mathbb{D}_i}^{\infty} = \bigcap_{j \in T_i} P_j.$$

Thus, since $\bigcup_{i=1}^{l} T_i = \{1, \ldots, l\}$, the following intersection

$$\bigcap_{i=1}^{l} [\mathbb{D}_i] : H_{\mathbb{D}_i}^{\infty}$$

is a characteristic decomposition of $I = P_1 \cap \ldots \cap P_l$ w.r.t. $\leq'$. This concludes the algebraic computation of a characteristic decomposition of I w.r.t. the target ranking, which we summarize in the Algorithm 8.

Now, in order to convert a characteristic decomposition

$$I = \bigcap_{i=1}^{p} [\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty}$$

of a radical differential ideal I w.r.t. $\leq$ to a ranking $\leq'$, one just applies Algorithm 8 to each characterizable component $[\mathbb{C}_i] : H_{\mathbb{C}_i}^{\infty}$ and then collects all the results together in a single intersection.

7. Conclusions

By estimating the orders of derivatives, we have shown that, given a set of ordinary differential polynomials specifying a radical differential ideal I, one can construct a Nötherian ring of algebraic polynomials, in which the computation of a characteristic decomposition of I is actually performed. This does not mean that the computation is

completely algebraic: differentiations are allowed, but they never lead out of the constructed algebraic ring.

For the problem of converting a characteristic decomposition of a radical differential ideal from one ranking to another, we have proposed an algorithm, which first differentiates the input polynomials sufficiently many times, and then performs the conversion completely algebraically, without using differentiation at all. The algorithm is applicable in the partial differential case, but the bound for the number of differentiations of the input polynomials is given for the ordinary case only.

We conjecture that, if one can solve the first problem of computing a characteristic decomposition of a radical differential ideal from generators completely algebraically, i.e., by an algorithm that first differentiates the input polynomials sufficiently many times, and then computes the decomposition without using differentiations, then one can also solve the Ritt problem of computing an irredundant prime (or characteristic) decomposition of a radical differential ideal.

Acknowledgements

We thank Michael F. Singer, François Boulier, William Sit, Évelyne Hubert, and Evgeniy Pankratiev for their important suggestions.

References

Boulier, F., 1999. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Tech. rep., Université Lille, presented at the MEGA-2000 Conference, Bath, England.

Boulier, F., 2001. Triangularisation de systèmes différentiels. Chapitre en Français pour l'ouvrage collectif de calcul formel. See: `http://www.lifl.fr/~Eboulier/PUBLICATIONS/triangularisation.ps.gz`.

Boulier, F., 2006. Réécriture algébrique dans les systèmes d'équations différentielles en vue d'applications dans les Sciences du Vivant. Mémoire d'Habilitation à Diriger des Recherches. See: `http://www.lifl.fr/~boulier/PUBLICATIONS/hdr.ps.gz`.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 1995. Representation for the radical of a finitely generated differential ideal. In: Proceedings of ISSAC 1995. ACM Press, pp. 158–166.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 1997. Computing representations for radicals of finitely generated differential ideals. Tech. rep., IT-306, LIFL.

Boulier, F., Lemaire, F., 2000. Computing canonical representatives of regular differential ideals. In: Proceedings of ISSAC 2000. ACM Press, pp. 38–47.

Boulier, F., Lemaire, F., Moreno-Maza, M., 2001. PARDI! In: Proceedings of ISSAC 2001. ACM Press, pp. 38–47.

Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the D5 principle. In: Proc. of *Transgressive Computing 2006*. University of Granada, Spain, pp. 79–92.

Bouziane, D., Kandri Rodi, A., Maârouf, H., 2001. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. Journal of Symbolic Computation 31, 631–649.

Cluzeau, T., Hubert, E., 2003. Resolvent representation for regular differential ideals. Applicable Algebra in Engineering, Communication and Computing 13 (5), 395–425.
Dahan, X., Jin, X., Moreno Maza, M., Schost, E., 2006. Change of ordering for regular chains in positive dimension. In: Kotsireas, I. (Ed.), Maple Conference'06. Maplesoft, pp. 26–43.
Gerdt, V. P., Blinkov, Y. A., 1998. Involutive bases of polynomial ideals. Mathematics and Computers in Simulation 45, 519–542.
Golubitsky, O., 2004. Gröbner walk for characteristic sets of prime differential ideals. In: Ganzha, V., Mayr, E., Vorozhtsov, E. (Eds.), Proceedings of the 7th Workshop on Computer Algebra in Scientific Computing. TU München, Germany, pp. 207–221.
Golubitsky, O., 2006. Universal characteristic sets of prime differential ideals. Journal of Symbolic Computation (to appear).
Golubitsky, O., Kondratieva, M., Ovchinnikov, A., 2005. Canonical characteristic sets of characterizable differential ideals (preprint).
Hubert, E., 2000. Factorization-free decomposition algorithms in differential algebra. Journal of Symbolic Computation 29 (4-5), 641–662.
Hubert, E., 2003. Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems. In: Symbolic and Numerical Scientific Computing 2001. pp. 40–87.
Hubert, E., 2004. Improvements to a triangulation-decomposition algorithm for ordinary differential systems in higher degree cases. In: Proceedings of ISSAC 2004. ACM Press, pp. 191–198.
Kolchin, E., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.
Kondratieva, M., Levin, A., Mikhalev, A., Pankratiev, E., 1999. Differential and difference dimension polynomials. Kluwer Academic Publisher.
Lemaire, F., Moreno Maza, M., Xie, Y., 2005. The `regularchains` library. In: Kotsireas, I. (Ed.), Maple Conference'05. Maplesoft, pp. 355–368.
Moreno Maza, M., 1999. On triangular decompositions of algebraic varieties. Tech. Rep. TR 4/99, NAG Ltd, Oxford, UK, presented at the MEGA-2000 Conference, Bath, England.
Moreno Maza, M., Xie, Y., 2006. Parallelization of triangular decomposition. In: Proc. of Algebraic Geometry and Geometric Modeling'06. University of Barcelona, Spain.
Morrison, S., 1999. The differential ideal $[P] : M^\infty$. Journal of Symbolic Computation 28, 631–656.
Ritt, J., 1950. Differential Algebra. American Mathematical Society, New York.
Sit, W., 2002. The Ritt-Kolchin theory for differential polynomials. In: Differential Algebra and Related Topics, Proceedings of the International Workshop (NJSU, 2–3 November 2000).
Szántó, Á., 1999. Computation with polynomial systems. Ph.D. thesis, Cornell University.